(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

**特開平11－328269**

(43)公開日　平成11年(1999)11月30日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 17/60 | | Ｇ０６Ｆ | 15/21 | Ｚ |
| Ｇ０７Ｆ | 7/08 | | Ｇ０７Ｇ | 1/12 | ３２１Ｍ |
| Ｇ０７Ｇ | 1/12 | ３２１ | Ｇ０９Ｃ | 1/00 | ６６０Ｚ |
| Ｇ０９Ｃ | 1/00 | ６６０ | Ｇ０７Ｆ | 7/08 | Ｍ |
| Ｈ０４Ｌ | 9/32 | | Ｈ０４Ｌ | 9/00 | ６７５Ｃ |

審査請求　未請求　請求項の数18　ＯＬ　（全 35 頁）

(21)出願番号　特願平10－133550

(22)出願日　平成10年(1998)５月15日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　梅澤　克之
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

最終頁に続く

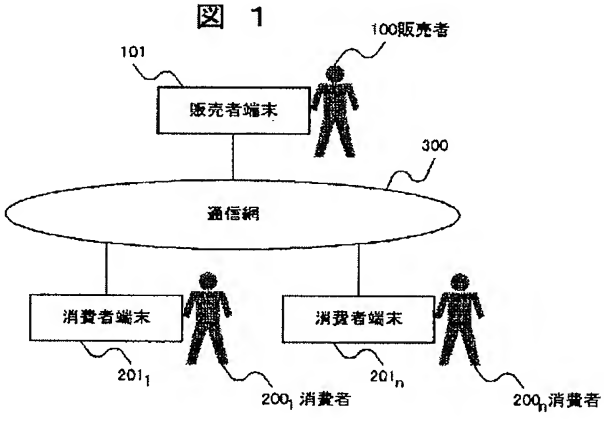
(54)【発明の名称】　電子クーポンシステムおよび電子クーポン発券・検証方法

(57)【要約】

【課題】電子的に発券されたクーポンを印刷して使用する場合でも、クーポンの偽造や改ざん，第三者によるクーポンの不正使用を検出することを可能とする。

【解決手段】クーポン発券時に、販売者１００は、消費者２００から送信されたパスワードの不可逆変換値と、改ざんされては困るクーポン情報と、クーポン情報のデジタル署名とを、印刷しても目視可能なデータとして記載したクーポンを作成するので、消費者２００がクーポンを印刷して使用する場合でも、クーポンに記載されているデジタル署名を検証することで、クーポンの改ざんや偽造を検出することができる。また、消費者２００は、クーポンの使用時に、発券時と同じパスワードを販売者１００に提示し、販売者１００は、提示されたパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較することで、第三者によるクーポンの不正使用を検出することができる。

図　1



【特許請求の範囲】

【請求項１】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末とが、ネットワークを介して相互に接続されてなり、
上記消費者端末は、
上記販売者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、
上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、
上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、
上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、
上記販売者端末は、
上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、
上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、
上記販売者端末のクーポン発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、
上記販売者端末のクーポン検証手段は、
上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、
該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、
上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、
印刷されたクーポンに記載されている不可逆変換値とクーポン情報と暗号化情報とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、取得した暗号化情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項２】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末とが、ネットワークを介して相互に接続されてなり、
上記消費者端末は、
上記販売者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、
上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、
上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、
上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、
上記販売者端末は、
上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、
上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、
上記販売者端末のクーポン発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果を、公開鍵暗号方式における販売者の秘密鍵を用いて暗号化したデジタル署名と、上記クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、
上記販売者端末のクーポン検証手段は、
上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、
該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、
上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、
印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得

られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項３】請求項１または２記載の電子クーポンシステムであって、

上記販売者端末のクーポン発券手段は、

作成したクーポンと共に、公開鍵暗号方式における販売者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信し、

上記消費者端末のクーポン受信手段は、

受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項４】請求項１，２または３記載の電子クーポンシステムであって、

上記クーポン情報は、クーポンごとに固有のシリアル番号を含み、

上記販売者端末は、

効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を記憶するシリアル番号記憶手段を備え、

上記販売者端末のクーポン検証手段は、

検証対象のクーポンに記載されているクーポン情報中のシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証することを特徴とする電子クーポンシステム。

【請求項５】請求項１，２，３または４記載の電子クーポンシステムであって、

上記消費者端末は、

上記販売者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記販売者端末は、

上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記販売者端末の初期チケット発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値$H_1$に基づいて、不可逆変換値$H_i$（$1 \leqq i < n$）の不可逆変換値$H_{i+1}$を順次計算し、上記ＵＩＤおよび不可逆変換値$H_n$を、１枚目のチケットとして、該消費者端末に対して送信し、

上記販売者端末のチケット発券手段は、

上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤと、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値$H_1$に基づいて、不可逆変換値$H_i$（$1 \leqq i < n$）の不可逆変換値$H_{i+1}$を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値$H_m$（$1 \leqq m \leqq n$）と、不可逆変換値$H_1$とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび不可逆変換値$H_{m-1}$を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。

【請求項６】請求項１，２，３または４記載の電子クーポンシステムであって、

上記消費者端末は、

上記販売者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記販売者端末は、

上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記販売者端末の初期チケット発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を計算すると共に、計算した暗号化情報$H_1$に基づい

て、暗号化情報$H_i$（$1 \leqq i < n$）の暗号化情報$H_{i+1}$を順次計算し、上記ＵＩＤおよび暗号化情報$H_n$を、１枚目のチケットとして、該消費者端末に対して送信し、
上記販売者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤとを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を計算すると共に、計算した暗号化情報$H_1$に基づいて、暗号化情報$H_i$（$1 \leqq i < n$）の暗号化情報$H_{i+1}$を順次計算し、受信した発券済み最新チケットのうちの暗号化情報$H_m$（$1 \leqq m \leqq n$）と、暗号化情報$H_1$とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび暗号化情報$H_{m-1}$を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項７】請求項１，２，３または４記載の電子クーポンシステムであって、
上記消費者端末は、
上記販売者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、
上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、
上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
上記販売者端末は、
上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
上記販売者端末の初期チケット発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、１枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を、１枚目のチケットとして、該消費者端末に対して送信し、
上記販売者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チケットである暗号化情報$H_m$（$1 \leqq m \leqq n$）を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、ｎ枚目のチケットである旨を示す枚数情報であるならば、ｎ枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報$H_m$（$1 \leqq m \leqq n$）を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られるＵＩＤと、ｍ＋１枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_{m+1}$を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項８】請求項１，２，３，４，５，６または７記載の電子クーポンシステムであって、
上記消費者端末は、
上記販売者端末に対してパスワードを送信する際には、公開鍵暗号方式における販売者の公開鍵を用いて該パスワードを暗号化してから送信し、
上記販売者端末は、
上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における販売者の秘密鍵を用いて該パスワードを復号することを特徴とする電子クーポンシステム。
【請求項９】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末と、発券者が利用する少なくとも１つの発券者端末とが、ネットワークを介して相互に接続されてなり、
上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、
上記発券者端末から送信されてくるクーポンを受信するクーポン受信手段と、
上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、
上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段を備え、
上記販売者端末は、
上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段を備え、
上記発券者端末のクーポン発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を公開鍵

暗号方式における発券者の秘密鍵を用いて暗号化したデジタル署名とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、
上記販売者端末のクーポン検証手段は、
上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、
上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、
印刷されたクーポンに記載されている不可逆変換値とクーポン情報とデジタル署名とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。
【請求項１０】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末と、発券者が利用する少なくとも１つの発券者端末とが、ネットワークを介して相互に接続されてなり、
上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、
上記発券者端末から送信されてくるクーポンを受信するクーポン受信手段と、
上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、
上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段を備え、
上記販売者端末は、
上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段を備え、
上記発券者端末のクーポン発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果を、公開鍵暗号方式における発券者の秘密鍵を用いて暗号化したデジタル署名と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、
上記販売者端末のクーポン検証手段は、
上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、
該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、
上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、
印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。
【請求項１１】請求項９または１０記載の電子クーポンシステムであって、
上記発券者端末のクーポン発券手段は、
作成したクーポンと共に、公開鍵暗号方式における発券者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信し、
上記消費者端末のクーポン受信手段は、
受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果とが一致するか否かを検証することを特徴とする電子クーポンシステム。
【請求項１２】請求項９，１０または１１記載の電子クーポンシステムであって、
上記クーポン情報は、クーポンごとに固有のシリアル番号を含み、
上記発券者端末は、
上記販売者端末から通知されたシリアル番号を記憶するシリアル番号記憶手段と、
上記販売者端末から問い合わせがあったシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証し、検証結果を該販売者端末に対して回答するシ

リアル番号検証手段とを備え、
上記販売者端末のクーポン検証手段は、
効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を、上記発券者端末に対して通知すると共に、検証対象のクーポンに記載されているクーポン情報中のシリアル番号についての検証結果を、上記発券者端末に対して問い合わせることを特徴とする電子クーポンシステム。
【請求項１３】請求項９，１０，１１または１２記載の電子クーポンシステムであって、
上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、
上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、
上記発券者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
上記発券者端末の初期チケット発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、発券者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値$H_1$に基づいて、不可逆変換値$H_i$（$1 \leqq i < n$）の不可逆変換値$H_{i+1}$を順次計算し、上記ＵＩＤおよび不可逆変換値$H_n$を、１枚目のチケットとして、該消費者端末に対して送信し、
上記発券者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤと、発券者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値$H_1$に基づいて、不可逆変換値$H_i$（$1 \leqq i < n$）の不可逆変換値$H_{i+1}$を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値$H_m$（$1 \leqq m \leqq n$）と、不可逆変換値$H_1$とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび不可逆変換値$H_{m-1}$を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項１４】請求項９，１０，１１または１２記載の電子クーポンシステムであって、
上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、
上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、
上記発券者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
上記発券者端末の初期チケット発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）とを連結し、発券者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を計算すると共に、計算した暗号化情報$H_1$に基づいて、暗号化情報$H_i$（$1 \leqq i < n$）の暗号化情報$H_{i+1}$を順次計算し、上記ＵＩＤおよび暗号化情報$H_n$を、１枚目のチケットとして、該消費者端末に対して送信し、
上記発券者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤとを連結し、発券者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を計算すると共に、計算した暗号化情報$H_1$に基づいて、暗号化情報$H_i$（$1 \leqq i < n$）の暗号化情報$H_{i+1}$を順次計算し、受信した発券済み最新チケットのうちの暗号化情報$H_m$（$1 \leqq m \leqq n$）と、暗号化情報$H_1$とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび暗号化情報$H_{m-1}$を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項１５】請求項９，１０，１１または１２記載の電子クーポンシステムであって、

上記消費者端末は、
上記発券者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、
上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、
上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
上記発券者端末は、
上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
上記発券者端末の初期チケット発券手段は、
上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、１枚目のチケットである旨を示す枚数情報とを連結し、発券者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を、１枚目のチケットとして、該消費者端末に対して送信し、
上記発券者端末のチケット発券手段は、
上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チケットである暗号化情報$H_m$（$1 \leqq m \leqq n$）を、発券者だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、ｎ枚目のチケットである旨を示す枚数情報であるならば、ｎ枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報$H_m$（$1 \leqq m \leqq n$）を、発券者だけしか知らない秘密の暗号鍵を用いて復号した結果得られるＵＩＤと、ｍ＋１枚目のチケットである旨を示す枚数情報とを連結し、発券者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_{m+1}$を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
【請求項１６】請求項９，１０，１１，１２，１３，１４または１５記載の電子クーポンシステムであって、
上記消費者端末は、
上記発券者端末に対してパスワードを送信する際には、公開鍵暗号方式における発券者の公開鍵を用いて該パスワードを暗号化してから送信し、また、上記販売者端末に対してパスワードを送信する際には、公開鍵暗号方式における販売者の公開鍵を用いて該パスワードを暗号化してから送信し、
上記発券者端末は、
上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における発券者の秘密鍵を用いて該パスワードを復号し、
上記販売者端末は、
上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における販売者の秘密鍵を用いて該パスワードを復号することを特徴とする電子クーポンシステム。
【請求項１７】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末とが、ネットワークを介して相互に接続されてなるシステムにおいて、１枚で予め定めた効力を発揮するクーポンの発券および検証を行う方法であって、
クーポンの発券時に、
上記販売者端末は、
クーポンの発券を要求した消費者端末から送信されてくるパスワードを受信し、受信したパスワードと、クーポンの効力に関するクーポン情報とを、自身だけしか暗号化できない暗号化方法で暗号化し、暗号化した結果である暗号化情報と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを消費者端末に対して送信し、
クーポンの検証時に、
上記販売者端末は、
検証対象のクーポンが、上記消費者端末から送信されて使用が要求されたクーポンである場合には、
該消費者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化し、暗号化した結果と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、
検証対象のクーポンが、上記消費者端末で印刷されて使用が要求されたクーポンである場合には、
印刷されたクーポンに記載されているクーポン情報および暗号化情報を取得し、消費者から提示されたパスワードおよび取得したクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化し、暗号化した結果と、取得した暗号化情報とが一致するか否かを検証することを特徴とする電子クーポン発券・検出方法。
【請求項１８】消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末と、発券者が利用する少なくとも１つの発券者端末とが、ネットワークを介して相互に接続されてなるシステムにおいて、１枚で予め定めた効力を発揮するクーポンの発券および検証を行う方法であって、
クーポンの発券時に、

上記発券者端末は、
クーポンの発券を要求した消費者端末から送信されてくるパスワードを受信し、受信したパスワードと、クーポンの効力に関するクーポン情報とを、自身だけしか暗号化できない暗号化方法で暗号化し、暗号化した結果である暗号化情報と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを消費者端末に対して送信し、
クーポンの検証時に、
上記販売者端末は、
検証対象のクーポンが、上記消費者端末から送信されて使用が要求されたクーポンである場合には、
該消費者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、上記発券者端末に対して送信して、該クーポンの検証を要求し、
検証対象のクーポンが、上記消費者端末で印刷されて使用が要求されたクーポンである場合には、
印刷されたクーポンを取得し、消費者から提示されたパスワードおよび取得したクーポンを、上記発券者端末に対して送信して、該クーポンの検証を要求し、
上記発券者端末は、
クーポンの検証を要求した販売者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化した結果と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、検証結果を該販売者端末に対して通知することを特徴とする電子クーポン発券・検出方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネット等のネットワークを介して行われる電子商取引システムの利用環境において、各種商品やサービスと交換可能な電子クーポンを適正に取り扱うための電子クーポンシステムに関し、さらに詳しくは、ネットワークを介して電子クーポンを受け取った消費者が、該電子クーポンを、ネットワーク上に開設されたバーチャル販売店だけではなく、現実に存在する販売店でも使用することができるようにした電子クーポンシステムに関する。

【０００２】

【従来の技術】現在、商品券や割引券等といった、各種商品やサービスと交換できる券（以下、総じて「クーポン」と称す。）が普及している。この種のクーポンには、１枚で効力を発揮するものと、複数枚だけ集めたときに効力を発揮するものとがあるが、効力が大きくなるほど、高度な印刷技術を用いることで偽造や改ざんを困難にするようにしたり、使用時に署名を確認することで第三者の不正使用を防止するようにしたりしている。

【０００３】ところで、近年の情報機器の発達と通信環境の整備により、インターネットのようなオープンなネットワークを介した電子商取引が盛んに行われるようになってきている。販売者は、ネットワーク上に仮想的な店舗を開設し、一般消費者に対して商品の販売を行う。

【０００４】このようなネットワークを介した電子商取引においても、消費者サービスの一環としてクーポン（電子クーポン）を取り扱いたいという要求が高まっている。しかし、電子クーポンを単なる画像データとした場合は、正規手順で電子クーポンを受け取った消費者が、その電子クーポンをコピーして何度も使用したり、また、他の消費者に配布したりすることが簡単にできてしまう。さらに、オープンなネットワーク経由で電子クーポンを配布することから、第三者に盗聴され不正使用されてしまうという恐れもある。

【０００５】このような不正行為を防止するための対策として、電子クーポンシステムにおいては、以下のような暗号技術が用いられている。

【０００６】第１の対策として、電子クーポンシステムにおいては、電子クーポンの偽造や改ざんを防止するために、電子クーポンに販売者（発券元）のデジタル署名を付加し、使用時にそのデジタル署名を確認するようにしている。デジタル署名技術は、例えば、「暗号理論入門：岡本栄司著，共立出版（１９９６）」の１３３頁～１３８頁に開示されている。この文献での非対称暗号（公開鍵暗号）による署名方法を簡単に説明すると、以下のようである。

【０００７】署名者は、署名したいメッセージ（または、メッセージのハッシュ値）を、署名者だけしか知らない秘密鍵を用いて暗号化することで、署名データを作成し、メッセージと署名データとをひとまとめにして検証者に渡す。検証者は、受け取った署名データを、上記秘密鍵に対応した公開鍵を用いて復号し、復号した結果と受け取ったメッセージとが一致していれば、上記署名者によって署名されたデータであると判断する。

【０００８】また、第２の対策として、電子クーポンシステムにおいては、電子クーポンの二重使用を防止するために、各電子クーポンにシリアル番号を付加し、使用時にそのシリアル番号をチェックすることで、未使用の電子クーポンであるか否かを確認するようにしている。

【０００９】さらに、第３の対策として、電子クーポンシステムにおいては、第三者による電子クーポンの不正使用を防止するために、メッセージを暗号化して送信するようにしている。メッセージを暗号化する方法としては、例えば、「ＯｐｅｎＤｅｓｉｇｎ（１９９６／６号Ｎｏ.１４）：ＣＱ出版社」の１０１頁～１１２頁に記載されているＳＳＬ（Secure Socket Layer）等が挙げられる。

【００１０】

【発明が解決しようとする課題】電子クーポンの発券から使用に至る全ての処理をネットワークを介して行うよ

うな電子クーポン専用のシステムの場合は、上述した全ての対策を講じるようにすることで、様々な不正行為を防止することができる。しかし、消費者の使い勝手を考慮すれば、消費者がネットワークを介して受け取った電子クーポンを紙に印刷し、従来の紙ベースのクーポンと同様に、販売店に持参して使用するような、紙クーポン・電子クーポン併用システムが好ましいが、そのようなシステムの場合には、電子クーポンに付加されたデジタル署名が印刷結果に反映されないことから、電子クーポンの偽造を防止することができない。

【００１１】また、使用済みシリアル番号を販売店で管理しておくことで、クーポンの二重使用を防止することはできるが、ネットワークを介して受け取った電子クーポンが消費者端末の記憶装置から盗まれた場合や、印刷されたクーポンが盗まれた場合には、そのクーポンを第三者に不正使用されてしまうと、正当な消費者がクーポンを使用することができなくなってしまう。

【００１２】さらに、複数枚だけ集めたときに効力を発揮するようなクーポン（以下、この種のクーポンを「チケット」と称す。）を取り扱う場合には、１枚で効力を発揮するクーポンに比べて発券枚数が多くなり、また、全ての消費者がチケットを集め終わるとは限らないので、消費者ごとに販売者側で管理するのは大変である。

【００１３】本発明は、上記事情に鑑みてなされたものであり、その目的は、ネットワークを介して電子クーポンを受け取った消費者が、該電子クーポンを、ネットワーク上に開設されたバーチャル販売店だけではなく、現実に存在する販売店でも使用することができるようにした電子クーポンシステムを提供することにある。

【００１４】また、本発明の他の目的は、チケットを取り扱う場合に、販売者の手間を減らすことができるようにした電子クーポンシステムを提供することにある。

【００１５】

【課題を解決するための手段】上記目的を達成するために、本発明は、第１の態様として、消費者が利用する少なくとも１つの消費者端末と、販売者が利用する少なくとも１つの販売者端末とが、ネットワークを介して相互に接続されてなり、上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、１枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、上記販売者端末は、上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、上記販売者端末のクーポン発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、上記販売者端末のクーポン検証手段は、上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、印刷されたクーポンに記載されている不可逆変換値とクーポン情報と暗号化情報とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、取得した暗号化情報とが一致するか否かを検証することを特徴とした電子クーポンシステムを提供している。

【００１６】第１の態様によれば、改ざんされては困るクーポン情報について、それを暗号化した暗号化情報を、目視可能なデータとして記載したクーポンを作成するようにしているので、消費者がクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されている暗号化情報を検証することで、クーポンの偽造や改ざんを防止することができるようになる。

【００１７】また、第１の態様によれば、クーポンの発券時に消費者が提示したパスワードについて、その不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしているので、クーポンの使用時に消費者が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較することで、第三者によるクーポンの不正使用を検出することができるようになる。

【００１８】なお、第１の態様において、上記販売者端末のクーポン発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果を、公開鍵暗号方式における販売者の秘密鍵を用いて暗号化したデジタル署名と、上記クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポ

ンを該消費者端末に対して送信するようにしてもよく、このようにした場合は、上記販売者端末のクーポン検証手段は、上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証するようにすることができる。

【００１９】さらに、第１の態様において、上記販売者端末のクーポン発券手段は、作成したクーポンと共に、公開鍵暗号方式における販売者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信するようにし、上記消費者端末のクーポン受信手段は、受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果とが一致するか否かを検証するようにしてもよい。

【００２０】このようにすれば、クーポンの使用時だけではなく、クーポンの発券時に、クーポンの発券を受けた消費者側で、受け取ったクーポンを検証することができるようになる。

【００２１】さらに、第１の態様において、上記クーポン情報が、クーポンごとに固有のシリアル番号を含むようにし、上記販売者端末は、効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を記憶するシリアル番号記憶手段を備えるようにし、上記販売者端末のクーポン検証手段は、検証対象のクーポンに記載されているクーポン情報中のシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証するようにしてもよい。

【００２２】このようにすれば、クーポンの偽造や改ざん、および、第三者によるクーポンの不正使用に加えて、クーポンの二重使用も防止することができるようになる。

【００２３】また、上記他の目的を達成するために、本発明は、第２の態様として、第１の態様において、上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、予め定めたｎ（ｎ＞１）枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、１枚目のチケットの発券を要求する初期チケット発券要求手段と、上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、２枚目以降のチケットの発券を要求するチケット発券要求手段と、上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、上記販売者端末は、上記消費者端末から発券が要求された１枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、上記消費者端末から発券が要求された２枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、上記販売者端末の初期チケット発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値$H_1$に基づいて、不可逆変換値$H_i$（$1 \leqq i < n$）の不可逆変換値$H_{i+1}$を順次計算し、上記ＵＩＤおよび不可逆変換値$H_n$を、１枚目のチケットとして、該消費者端末に対して送信し、上記販売者端末のチケット発券手段は、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤと、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値$H_1$に基づいて、不可逆変換値$H_i$（$1 \leqq i < n$）の不可逆変換値$H_{i+1}$を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値$H_m$（$1 \leqq m \leqq n$）と、不可逆変換値$H_1$とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび不可逆変換値$H_{m-1}$を、次のチケットとして、該消費者端末に対して送信することを特徴とした電子クーポンシステムを提供している。

【００２４】第２の態様によれば、消費者だけしか知らない情報であるパスワードと、販売者だけしか知らない秘密の情報（例えば、公開鍵暗号方式における販売者の秘密鍵）と、ｎ枚のチケットの組を識別するためのＵＩＤとを連結したものから、不可逆変換値を繰り返し計算し、ｎ番目の計算結果，ｎ－１番目の計算結果，…，２番目の計算結果，１番目の計算結果という順番で、各計算結果をチケットとして発券するようにしているので、販売店側で、消費者ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【００２５】なお、第２の態様において、上記販売者端

末の初期チケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を計算すると共に、計算した暗号化情報$H_1$に基づいて、暗号化情報$H_i$（$1 \leqq i < n$）の暗号化情報$H_{i+1}$を順次計算し、上記ＵＩＤおよび暗号化情報$H_n$を、１枚目のチケットとして、該消費者端末に対して送信するようにし、上記販売者端末のチケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのＵＩＤとを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を計算すると共に、計算した暗号化情報$H_1$に基づいて、暗号化情報$H_i$（$1 \leqq i < n$）の暗号化情報$H_{i+1}$を順次計算し、受信した発券済み最新チケットのうちの暗号化情報$H_m$（$1 \leqq m \leqq n$）と、暗号化情報$H_1$とが一致したならば、ｎ枚のチケットの発券を完了し、一致しないならば、上記ＵＩＤおよび暗号化情報$H_{m-1}$を、次のチケットとして、該消費者端末に対して送信するようにしてもよい。

【００２６】また、第２の態様において、上記販売者端末の初期チケット発券手段は、上述した動作ではなく、上記販売者端末の初期チケット発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）と、１枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_1$を、１枚目のチケットとして、該消費者端末に対して送信するようにし、上記販売者端末のチケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チケットである暗号化情報$H_m$（$1 \leqq m \leqq n$）を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、ｎ枚目のチケットである旨を示す枚数情報であるならば、ｎ枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報$H_m$（$1 \leqq m \leqq n$）を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られるＵＩＤと、ｍ＋１枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報$H_{m+1}$を、次のチケットとして、該消費者端末に対して送信するようにしてもよい。

【００２７】【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【００２８】なお、以下の説明で参照する図面において、同一の符号は、同様の構成要素を表すものとする。また、これにより本発明が限定されるものではない。

【００２９】（第１の実施形態）まず、本発明の第１の実施形態について説明する。

【００３０】図１は、第１の実施形態に係る電子クーポンシステムの概略構成を示す図である。

【００３１】第１の実施形態に係る電子クーポンシステムは、消費者$200_1$～$200_n$（以下、単に「消費者２００」とも称す。）および販売者１００が利用するシステムであり、図１に示すように、消費者２００が利用する端末である消費者端末$201_1$～$201_n$（以下、単に「消費者端末２０１」とも称す。）と、販売者１００が利用する端末である販売者端末１０１とが、インターネット等の通信網３００を介して互いに接続されて構成されている。

【００３２】第１の実施形態に係る電子クーポンシステムにおいては、消費者２００が、消費者端末２０１を利用して、通信網３００を介して販売者端末１０１との間でデータをやり取りすることで、販売者１００に対してクーポンの発券を要求したり、販売者１００によって発券されたクーポンの使用を要求したりすることができるようにしている。このとき、販売者１００は、販売者端末１０１を利用して、消費者２００に対してクーポンを発券したり、消費者２００によって使用されるクーポンを検証したりする。

【００３３】特に、第１の実施形態に係る電子クーポンシステムにおいては、消費者２００が、消費者端末２０１を利用して、販売者１００によって発券されたクーポンを印刷し、印刷したクーポンを販売店に持参することで、直接、販売者１００に対してクーポンの使用を要求することもできるようにしている。このとき、販売者１００は、販売者端末１０１を利用して、消費者２００が持参したクーポンを検証する。

【００３４】すなわち、第１の実施形態に係る電子クーポンシステムは、通信網３００を介して行われる電子商取引環境を実現すると共に、消費者２００が、販売者１００によって発券されたクーポンを、通信網３００上に開設されたバーチャル販売店だけではなく、現実に存在する販売店でも使用することができるようにしたものである。

【００３５】次に、第１の実施形態に係る電子クーポンシステムを構成する販売者端末１０１および消費者端末２０１のハードウェア構成について、図２および図３を用いて説明する。

【００３６】図２は販売者端末１０１のハードウェア構成を示す図である。

【００３７】図２に示すように、販売者端末１０１は、

通信インタフェース１０２と、表示装置１０３と、入力装置１０４と、記憶装置１０５と、中央処理装置（ＣＰＵ）１０６と、一時記憶装置（メモリ）１０７とが、バス１１０によって互いに接続された構成となっている。

【００３８】通信インタフェース１０２は、通信網３００を介して、消費者端末２０１との間でデータのやり取りを行うためのインタフェースである。

【００３９】また、表示装置１０３は、販売者端末１０１を利用する販売者１００に対するメッセージ等を表示するために用いられるものであり、ＣＲＴや液晶ディスプレイ等で構成される。

【００４０】また、入力装置１０４は、販売者端末１０１を利用する販売者１００がデータや命令等を入力するために用いられるものであり、キーボードやマウス等で構成される。

【００４１】また、記憶装置１０５は、販売者端末１０１で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【００４２】また、ＣＰＵ１０６は、販売者端末１０１の構成要素を統括的に制御したり、様々な演算処理を行ったりする。

【００４３】また、メモリ１０７には、オペレーティングシステム（以下、「ＯＳ」と称す。）１０７ａや、クーポン発券・検証処理プログラム１０７ｂといった、ＣＰＵ１０６が実行するプログラム等が一時的に格納される。

【００４４】ここで、ＯＳ１０７ａは、販売者端末１０１全体の制御を行うために、ファイル管理，プロセス管理，デバイス管理といった機能を実現するためのプログラムである。また、クーポン発券・検証処理プログラム１０７ｂは、消費者２００に対してクーポンを発券したり、消費者２００から使用が要求されたクーポンを検証したりするためのプログラムである。

【００４５】図３は消費者端末２０１のハードウェア構成を示す図である。

【００４６】図３に示すように、消費者端末２０１は、通信インタフェース２０２と、表示装置２０３と、入力装置２０４と、記憶装置２０５と、中央処理装置（ＣＰＵ）２０６と、一時記憶装置（メモリ）２０７と、印刷装置２０８とが、バス２１０によって互いに接続された構成となっている。

【００４７】通信インタフェース２０２は、通信網３００を介して、販売者端末１０１との間でデータのやり取りを行うためのインタフェースである。

【００４８】また、表示装置２０３は、消費者端末２０１を利用する消費者２００に対するメッセージ等を表示するために用いられるものであり、ＣＲＴや液晶ディスプレイ等で構成される。

【００４９】また、入力装置２０４は、消費者端末２０１を利用する消費者２００がデータや命令等を入力するために用いられるものであり、キーボードやマウス等で構成される。

【００５０】また、記憶装置２０５は、消費者端末２０１で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【００５１】また、ＣＰＵ２０６は、消費者端末２０１の構成要素を統括的に制御したり、様々な演算処理を行ったりする。

【００５２】また、メモリ２０７には、ＯＳ２０７ａや、クーポン要求・受信・発信処理プログラム２０７ｂといった、ＣＰＵ２０６が実行するプログラム等が一時的に格納される。

【００５３】ここで、ＯＳ２０７ａは、消費者端末２０１全体の制御を行うために、ファイル管理，プロセス管理，デバイス管理といった機能を実現するためのプログラムである。また、クーポン要求・受信・発信処理プログラム２０７ｂは、販売者１００に対してクーポンの発券を要求したり、販売者１００によって発券されたクーポンを受信したり、販売者１００に対してクーポンの使用を要求したりするためのプログラムである。

【００５４】また、印刷装置２０８は、電子的なデータを印刷するために用いられるものであり、プリンタ等で構成される。

【００５５】次に、第１の実施形態に係る電子クーポンシステムの動作について説明する。

【００５６】なお、以下の説明おいて、消費者２００が行う処理は、実際には、消費者２００の指示によって消費者端末２０１が実行し、販売者１００が行う処理は、実際には、販売者１００の指示によって販売者端末１０１が実行するものである。

【００５７】図４は、消費者２００が、販売者１００に対してクーポンの発券を要求し、販売者１００によって発券されたクーポンを受信するまでの動作を説明するための図である。

【００５８】図４において、まず、消費者２００は、販売者１００からクーポンの発券を受ける条件を満たしているものとする（Ｓ２０００）。

【００５９】消費者２００は、後述するクーポン要求処理（Ｓ２４００）を行い、暗号化した自身のパスワード５０１を、販売者１００に対して送信する。

【００６０】販売者１００は、パスワード５０１を受信すると、後述するクーポン発券処理（Ｓ１３００）を行い、クーポン５０２と、クーポン５０２のデジタル署名５０３とを、消費者２００に対して送信する。

【００６１】消費者２００は、クーポン５０２およびデジタル署名５０３を受信すると、後述するクーポン受信処理（Ｓ２５００）を行い、受信したクーポン５０２を保管する。

【００６２】図５は、既にクーポンの発券を受けている消費者２００が、通信網３００を介してクーポンを使用し、販売者１００が、クーポンを検証するまでの動作を説明するための図である。

【００６３】図５において、既にクーポンの発券を受けている消費者２００は、後述するクーポン使用オンライン処理（Ｓ２６００）を行い、クーポン受信処理（Ｓ２５００）で入手したクーポン５０２と、暗号化した自身のパスワード５０１とを、販売者１００に対して送信する。

【００６４】販売者１００は、クーポン５０２およびパスワード５０１を受信すると、後述するクーポン検証処理（Ｓ１４００）を行い、受信したクーポン５０２を検証する。

【００６５】図６は、既にクーポンの発券を受けている消費者２００が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者１００が、クーポンを検証するまでの動作を説明するための図である。

【００６６】図６において、既にクーポンの発券を受けている消費者２００は、後述するクーポン使用オフライン処理（Ｓ２７００）を行い、印刷されたクーポン５０４を販売店に持参する。

【００６７】販売者１００は、消費者２００が持参したクーポン５０４を受け取ると、クーポン検証処理（Ｓ１４００）を行い、受け取ったクーポン５０４を検証する。

【００６８】図７は、図４のクーポン要求処理（Ｓ２４００）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム２０７ｂによって実現される。

【００６９】図７に示すように、クーポン要求処理（Ｓ２４００）において、消費者２００は、まず、販売者１００に対して、公開鍵暗号方式における販売者１００の公開鍵を要求し、公開鍵を受信する（ステップ２４０１）。

【００７０】続いて、消費者２００は、自身だけしか知らないパスワードを入力する（ステップ２４０２）。

【００７１】続いて、消費者２００は、ステップ２４０２で入力したパスワードを、ステップ２４０１で入手した公開鍵を用いて暗号化し（ステップ２４０３）、暗号化したパスワード５０１を、販売者１００に対して送信する（ステップ２４０４）。

【００７２】図８は、図４のクーポン発券処理（Ｓ１３００）の処理フローチャートであり、本処理は、クーポン発券・検証処理プログラム１０７ｂによって実現される。

【００７３】図８に示すように、クーポン発券処理（Ｓ１３００）において、販売者１００は、まず、暗号化されたパスワード５０１を受信すると（ステップ１３０１）、受信したパスワード５０１を、公開鍵暗号方式における販売者１００の秘密鍵を用いて復号する（ステップ１３０２）。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網３００を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【００７４】続いて、販売者１００は、ステップ１３０２で復号したパスワード５０１に不可逆変換を施す（ステップ１３０３）。以下、パスワードに不可逆変換を施した結果を、パスワードの不可逆変換値またはＰＨと称す。

【００７５】続いて、販売者１００は、シリアル番号，有効期限，クーポンの価値（例えば、金額）等の、クーポンの効力に関するクーポン情報を設定し（ステップ１３０４）、設定したクーポン情報のデジタル署名を、販売者１００の秘密鍵を用いて計算する（ステップ１３０５）。そして、ステップ１３０３で計算した不可逆変換値，ステップ１３０４で設定したクーポン情報，ステップ１３０５で計算したデジタル署名を、目視可能なデータ（例えば、数字や文字等）として記載したクーポンを作成することで、書面としてのクーポン５０２を作成する（ステップ１３０６）。

【００７６】続いて、販売者１００は、書面としてのクーポン５０２全体のデジタル署名５０３を、販売者１００の秘密鍵を用いて計算し（ステップ１３０７）、ステップ１３０６で作成したクーポン５０２と、ステップ１３０７で計算したデジタル署名５０３とを、消費者２００に対して送信する（ステップ１３０８）。

【００７７】図９は、図４のクーポン受信処理（Ｓ２５００）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム２０７ｂによって実現される。

【００７８】図９に示すように、クーポン受信処理（Ｓ２５００）において、消費者２００は、販売者１００が送信したクーポン５０２およびデジタル署名５０３を受信すると（ステップ２５０１）、受信したデジタル署名５０３を検証することで、受信したクーポン５０２が、通信網３００を介して送信されてくる間に改ざんされていないか否かを検証する（ステップ２５０２）。ステップ２５０２では、詳しくは、消費者２００は、受信したクーポン５０２と、受信したデジタル署名５０３を販売者１００の公開鍵を用いて復号した結果とを比較し、両者が一致すれば、受信したクーポン５０２が改ざんされていないと判断する。

【００７９】そして、改ざんされていないならば、受信したクーポン５０２を記憶装置２０５に保存する（ステップ２５０３）。

【００８０】ここで、クーポン５０２は、例えば、図１４に示すような形式とすることができ、受信時に表示装置２０３に表示されるようにすることが好ましい。

【００８１】図１０は、図５のクーポン使用オンライン

処理（Ｓ２６００）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム２０７ｂによって実現される。

【００８２】図１０に示すように、クーポン使用オンライン処理（Ｓ２６００）において、消費者２００は、まず、販売者１００に対して、販売者１００の公開鍵を要求し、公開鍵を受信する（ステップ２６０１）。

【００８３】続いて、消費者２００は、自身だけしか知らないパスワード（クーポン要求処理（Ｓ２４００）で入力したパスワードと同一のパスワード）を入力する（ステップ２６０２）。

【００８４】続いて、消費者２００は、ステップ２６０２で入力したパスワードを、ステップ２６０１で入手した公開鍵を用いて暗号化し（ステップ２６０３）、暗号化したパスワード５０１と、図９に示したクーポン受信処理（Ｓ２５００）で入手したクーポン５０２とを、販売者１００に対して送信する（ステップ２６０４）。

【００８５】図１１は、図６のクーポン使用オフライン処理（Ｓ２７００）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム２０７ｂによって実現される。

【００８６】図１１に示すように、クーポン使用オフライン処理（Ｓ２７００）において、消費者２００は、図９に示したクーポン受信処理（Ｓ２５００）で入手したクーポン５０２を、印刷装置２０８で印刷する（ステップ２７０１）。

【００８７】ここで、印刷されたクーポン５０４の形式は、図１４に示したクーポン５０２の形式と同様の形式である。

【００８８】続いて、消費者２００は、印刷されたクーポン５０４を販売店に持参し、自身だけしか知らないパスワード（クーポン要求処理（Ｓ２４００）で入力したパスワードと同一のパスワード）を、販売者１００に告げる（ステップ２７０２）。なお、ステップ２７０２は、消費者２００自身が行う行動であり、消費者端末２０１では実行されない。

【００８９】図１２は、図５および図６のクーポン検証処理（Ｓ１４００）の処理フローチャートであり、本処理は、クーポン発券・検証処理プログラム１０７ｂによって実現される。

【００９０】図１２に示すように、クーポン検証処理（Ｓ１４００）は、使用されるクーポンが、通信網３００を介してオンラインで届いたクーポン５０２であるか、または、直接持参されたクーポン（印刷されたクーポン）５０４であるかによって、処理が分かれる（ステップ１４０１）。

【００９１】直接持参されたクーポン５０４である場合には、販売者１００は、ステップ１４０４の書面検証処理から処理を開始する。ただし、このとき、販売者１００は、クーポン５０４に記載されている各種情報を取得する必要があるが、取得方法については任意である。

【００９２】また、通信網３００を介してオンラインで届いたクーポン５０２である場合には、販売者１００は、このクーポン５０２と共に、暗号化されたパスワード５０１を受信し（ステップ１４０２）、受信したパスワード５０１を、販売者１００の秘密鍵を用いて復号する（ステップ１４０３）。

【００９３】ステップ１４０４では、販売者１００は、クーポンに記載されている各種情報を検証する書面検証処理を行う。なお、書面検証処理の詳細については後述する。

【００９４】ステップ１４０４の書面検証処理の結果、全ての情報についての検証に合格した場合には（ステップ１４０５）、クーポンの二重使用を防止するために、クーポンに記載されているクーポン情報中のシリアル番号を、使用済みシリアル番号リストに登録し（ステップ１４０６）、クーポンの定められた効力を発揮させる（ステップ１４０７）。また、１つでも不合格であった場合には（ステップ１４０５）、エラー処理を実行する（ステップ１４０８）。

【００９５】図１３は、図１２の書面検証処理（ステップ１４０４）の処理フローチャートである。

【００９６】図１３に示すように、書面検証処理（ステップ１４０４）において、販売者１００は、まず、書面としてのクーポンに記載されているクーポン情報のデジタル署名を、販売者１００の秘密鍵を用いて計算する（ステップ１４１０）。

【００９７】そして、検証に合格しなければ（ステップ１４１１）、すなわち、計算したデジタル署名と、クーポンに記載されているデジタル署名とが一致しなければ、クーポンが改ざんされているので、エラー処理を実行する（ステップ１４１７）。

【００９８】また、検証に合格すれば（ステップ１４１１）、すなわち、計算したデジタル署名と、クーポンに記載されているデジタル署名とが一致すれば、ステップ１４０３で得たパスワード（または、消費者２００から告げられたパスワード）の不可逆変換値を計算し、計算した不可逆変換値と、書面としてのクーポンに記載されている不可逆変換値と比較する（ステップ１４１２）。

【００９９】ステップ１４１２の比較の結果、両者が一致しなければ（ステップ１４１３）、クーポン発券時のパスワードを知らない第三者によるクーポンの不正使用であると考えられるので、エラー処理を実行する（ステップ１４１８）。

【０１００】また、販売者１００は、書面としてのクーポンに記載されているクーポン情報中のシリアル番号が、使用済みシリアル番号リストに登録されているか否かを検証する（ステップ１４１４）。既に登録されているならば（ステップ１４１５）、クーポンの二重使用という理由で、エラー処理を実行する（ステップ１４１

９）。

【０１０１】最後に、販売者１００は、書面としてのクーポンに記載されているクーポン情報中の有効期限を参照し、有効期限内のクーポンであるか否かを検証し（ステップ１４１６）、有効期限外であれば、有効期限切れのエラー処理を実行する（ステップ１４２０）。

【０１０２】これら全ての検証に合格すれば、クーポンは有効となり、効力が発揮されることとなる。

【０１０３】以上説明したように、第１の実施形態に係る電子クーポンシステムにおいては、シリアル番号，有効期限，金額等の改ざんされては困るクーポン情報のデジタル署名を、販売者１００だけしか知らない情報である秘密鍵を用いて計算し、計算したデジタル署名を、目視可能なデータとして記載したクーポンを作成するようにしている。

【０１０４】従って、第１の実施形態に係る電子クーポンシステムによれば、消費者２００が電子的なクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されているデジタル署名を検証することで、クーポンの偽造や改ざんを検出することができる。

【０１０５】また、第１の実施形態に係る電子クーポンシステムにおいては、クーポンの発券時に、消費者２００が提示したパスワードの不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしている。さらに、クーポンの使用時には、発券を要求した消費者２００だけしか知らないパスワードを販売者１００に提示し、消費者２００が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較するようにしている。

【０１０６】従って、第１の実施形態に係る電子クーポンシステムによれば、たとえクーポンが盗まれたとしても、クーポンの発券要求時に提示されたパスワードを知らない第三者がクーポンを不正使用するのを防止することができる。

【０１０７】なお、第１の実施形態に係る電子クーポンシステムにおいては、クーポン情報について、公開鍵暗号方式における販売者１００の秘密鍵を用いて計算したデジタル署名を、目視可能なデータとしてクーポンに記載するようにした例を示しているが、販売者１００だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにしてもよい。

【０１０８】また、第１の実施形態に係る電子クーポンシステムにおいては、パスワードについて、不可逆変換を施した不可逆変換値を、目視可能なデータとしてクーポンに記載するようにした例を示しており、本例によれば、不可逆変換方法を公開しても支障がないので、パスワードの不可逆変換値が不一致である場合に、消費者２００が、自身が提示したパスワードの不可逆変換値を計算して確認することが可能である。しかしながら、パスワードについて、販売者１００だけしか暗号化できない暗号化方法で暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにしてもよい。

【０１０９】なお、本発明は、上述した第１の実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

【０１１０】例えば、第１の実施形態に係る電子クーポンシステムにおいては、消費者２００は、販売者１００に対してパスワードを送信するときに、販売者１００の公開鍵を取得し、暗号通信を行うようにしているが、本発明はこれに限定しない。消費者２００は、１度、販売者１００の公開鍵を入手すれば、２回以降は、その公開鍵を使うことができる。また、販売者１００と消費者２００との間で共通の鍵を持つことができれば、秘密鍵暗号技術を使って暗号化するようにしてもよい。

【０１１１】また、第１の実施形態に係る電子クーポンシステムにおいて、消費者２００から販売者１００に対してパスワードを送信するときに、暗号化されたパスワードがそのまま盗まれて不正使用されるのを防止するために、パスワードを、その他の情報（乱数や適当な数字でよい。）と共に暗号化して送信するようにしてもよい。

【０１１２】また、第１の実施形態に係る電子クーポンシステムにおいては、販売者１００は、デジタル署名を、数値や文字等の目視可能なデータとしてクーポンに記載するようにしているが、印刷後に目視可能であれば、例えば、バーコード等のようなものであってもよい。バーコードとして記載すれば、販売者１００は、印刷されたクーポンから各種情報を取得する際に、バーコードリーダを用いることができるようになる。

【０１１３】また、第１の実施形態に係る電子クーポンシステムにおいては、販売者１００は、消費者２００のパスワードの不可逆変換値と、シリアル番号，有効期限，金額等のクーポン情報のデジタル署名とを、別々にクーポンに記載するようにしているが、クーポン情報と共に、パスワードも一緒にデジタル署名を計算するようにしてもよい。また、このとき、クーポン情報やパスワード等の、デジタル署名を計算する元の情報は、不可逆変換を施した後に、デジタル署名を計算するようにしてもよい。

【０１１４】（第２の実施形態）ところで、クーポンは、販売者１００の販売方針により、１枚で効力を発揮するものと、ある種の条件を満たしたときのみ、効力を発揮するものとがある。例えば、予め定めた枚数だけ集めたときに効力を発揮するようなクーポン（以下、この種のクーポンを、特に「チケット」と称す。）を取り扱うようにした場合を、第２の実施形態として、上述した第１の実施形態と異なる点についてのみ説明する。

【０１１５】第２の実施形態に係る電子クーポンシステ

ムの概略構成は、図１に示した概略構成と同様である。

【０１１６】図１５は販売者端末１０１のハードウェア構成を示す図である。

【０１１７】図２に示したハードウェア構成と異なる点は、メモリ１０７に、チケット発券・検証処理プログラム１０７ｃが一時的に格納される点である。

【０１１８】チケット発券・検証処理プログラム１０７ｃは、消費者２００に対してチケットを発券したり、消費者２００から使用が要求されたチケットを検証したりするためのプログラムである。

【０１１９】図１６は消費者端末２０１のハードウェア構成を示す図である。

【０１２０】図３に示したハードウェア構成と異なる点は、メモリ２０７に、チケット要求・受信・発信処理プログラム２０７ｃが一時的に格納される点である。

【０１２１】チケット要求・受信・発信処理プログラム２０７ｃは、販売者１００に対してチケットの発券を要求したり、販売者１００によって発券されたチケットを受信したり、販売者１００に対してチケットの使用を要求したりするためのプログラムである。

【０１２２】次に、第２の実施形態に係る電子クーポンシステムの動作について説明する。

【０１２３】なお、以下の説明おいても、上述した第１の実施形態と同様に、消費者２００が行う処理は、実際には、消費者２００の指示によって消費者端末２０１が実行し、販売者１００が行う処理は、実際には、販売者１００の指示によって販売者端末１０１が実行するものである。

【０１２４】図１７は、消費者２００が、販売者１００に対して１枚目のチケットの発券を要求し、販売者１００によって発券された１枚目のチケットを受信するまでの動作を説明するための図である。なお、チケットは、ｎ枚だけ集めたときに効力を発揮するものとする。

【０１２５】図１７において、まず、消費者２００は、後述する初期チケット発券要求処理（Ｓ２１００）を行い、暗号化した自身のパスワード５０１を、販売者１００に対して送信する。

【０１２６】販売者１００は、パスワード５０１を受信すると、後述する初期チケット発券処理（Ｓ１１００）を行い、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）５０５と、受信したパスワード５０１，ＵＩＤ５０５，販売者１００だけしか知らない秘密の情報（例えば、販売者１００の秘密鍵）を連結したものの、ｎ番目の不可逆変換値$H_n$(５０６$_n$)とを、１枚目のチケットとして、消費者２００に対して送信する。

【０１２７】消費者２００は、ＵＩＤ５０５および$H_n$(５０６$_n$)を受信すると、後述するチケット受信処理（Ｓ２２００）を行い、受信したＵＩＤ５０５および$H_n$(５０６$_n$)を保管する。

【０１２８】図１８は、消費者２００が、販売者１００に対して２枚目以降のチケットの発券を要求し、販売者１００によって発券された２枚目以降のチケットを受信するまでの動作を説明するための図である。

【０１２９】図１８において、まず、消費者２００は、２枚目のチケットの発券を受ける場合は、後述するチケット発券要求処理（Ｓ２３００）を行い、暗号化した自身のパスワード５０１と、１枚目のチケット受信処理（Ｓ２２００）で入手したＵＩＤ５０５および$H_n$(５０６$_n$)とを、販売者１００に対して送信する。

【０１３０】販売者１００は、パスワード５０１，ＵＩＤ５０５，$H_n$(５０６$_n$)を受信すると、後述するチケット発券処理（Ｓ１２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，$H_n$(５０６$_n$)と、販売者１００の秘密鍵とから、$H_{n-1}$(５０６$_{n-1}$)を求めて、求めた$H_{n-1}$(５０６$_{n-1}$)を、２枚目のチケットとして、消費者２００に対して送信する。

【０１３１】消費者２００は、$H_{n-1}$(５０６$_{n-1}$)を受信すると、チケット受信処理（Ｓ２２００）を行い、受信した$H_{n-1}$(５０６$_{n-1}$)を保管する。

【０１３２】同様に、消費者２００は、ｍ＋１枚目（１≦ｍ＜ｎ）のチケットの発券を受ける場合は、チケット発券要求処理（Ｓ２３００）を行い、暗号化した自身のパスワード５０１と、ｍ枚目のチケット受信処理（Ｓ２２００）で入手したＵＩＤ５０５および$H_{n-(m-1)}$(５０６$_{n-(m-1)}$)とを、販売者１００に対して送信する。

【０１３３】販売者１００は、パスワード５０１，ＵＩＤ５０５，$H_{n-(m-1)}$(５０６$_{n-(m-1)}$)を受信すると、チケット発券処理（Ｓ１２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，$H_{n-(m-1)}$(５０６$_{n-(m-1)}$)と、販売者１００の秘密鍵とから、$H_{n-m}$(５０６$_{n-m}$)を求めて、求めた$H_{n-m}$(５０６$_{n-m}$)を、ｍ＋１枚目のチケットとして、消費者２００に対して送信する。

【０１３４】消費者２００は、$H_{n-m}$(５０６$_{n-m}$)を受信すると、チケット受信処理（Ｓ２２００）を行い、受信した$H_{n-m}$(５０６$_{n-m}$)を保管する。

【０１３５】このようにして、消費者２００は、ｎ枚のチケットを集めることができ、これらｎ枚のチケットの効力を発揮させたい場合には、チケット発券要求処理（Ｓ２３００）を行い、暗号化された自身のパスワード５０１と、ｎ枚目のチケット受信処理（Ｓ２２００）で入手したＵＩＤ５０５および$H_1$(５０６$_1$)とを、販売者１００に対して送信する。

【０１３６】販売者１００は、パスワード５０１，ＵＩＤ５０５，$H_1$(５０６$_1$)を受信すると、チケット発券処理（Ｓ１２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，$H_1$(５０６$_1$)と、販売者１００の秘密鍵とから、消費者２００がｎ枚だけチケットを集めたことを確認し、ｎ枚のチケット収集終了処理（Ｓ１２５０）を行う。

【０１３７】図１９は、図１７の初期チケット発券要求処理（Ｓ２１００）の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム２０７ｃによって実現される。

【０１３８】図１９に示すように、初期チケット発券要求処理（Ｓ２１００）において、消費者２００は、まず、販売者１００に対して、販売者１００の公開鍵を要求し、公開鍵を受信する（ステップ２１０１）。

【０１３９】続いて、消費者２００は、自身だけしか知らないパスワードを入力する（ステップ２１０２）。

【０１４０】続いて、消費者２００は、ステップ２１０２で入力したパスワードを、ステップ２１０１で入手した公開鍵を用いて暗号化し（ステップ２１０３）、暗号化したパスワード５０１を、販売者１００に対して送信する（ステップ２１０４）。

【０１４１】図２０は、図１７の初期チケット発券処理（Ｓ１１００）の処理フローチャートであり、本処理は、チケット発券・検証処理プログラム１０７ｃによって実現される。

【０１４２】図２０に示すように、初期チケット発券処理（Ｓ１１００）において、販売者１００は、まず、暗号化されたパスワード５０１を受信すると（ステップ１１０１）、受信したパスワード５０１を、販売者１００の秘密鍵を用いて復号する（ステップ１１０２）。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網３００を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【０１４３】続いて、販売者１００は、ｎ枚のチケットの組を識別するための固有の値であるＵＩＤ５０５を作成し（ステップ１１０３）、ステップ１１０２で復号したパスワード，ステップ１１０３で作成したＵＩＤ５０５，販売者１００の秘密鍵を結合したものに、不可逆変換を施す（ステップ１１０４）。以下、パスワード，ＵＩＤ，秘密鍵を結合したものに不可逆変換を施した結果を、不可逆変換値$H_m$（$1 \leqq m \leqq n$）と称すが、ステップ１１０４で計算される不可逆変換値$H_m$は$H_1$($506_1$)である。

【０１４４】続いて、販売者１００は、$H_i$の不可逆変換値$H_{i+1}$（$1 \leqq i < n$）を計算する（ステップ１１０５）。ステップ１１０５では、詳しくは、販売者１００は、図２４に示すように、まず、$H_1$($506_1$)の不可逆変換値$H_2$($506_2$)を計算し、$H_{n-1}$($506_{n-1}$)の不可逆変換値$H_n$($506_n$)を計算するまで、$H_i$の不可逆変換値$H_{i+1}$（$1 \leqq i < n$）を繰り返し計算する。

【０１４５】最後に、販売者１００は、ステップ１１０３で作成したＵＩＤ５０５と、ｎ番目の不可逆変換値$H_n$（$506_n$)とを、１枚目のチケットとして、消費者２００に対して送信する（ステップ１１０６）。

【０１４６】図２１は、図１７および図１８のチケット受信処理（Ｓ２２００）の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム２０７ｃによって実現される。

【０１４７】図２１に示すように、チケット受信処理（Ｓ２２００）において、消費者２００は、販売者１００から送信されてきたデータを受信すると（ステップ２２０１）、受信したデータにＵＩＤ５０５が含まれているか否かを判定し（ステップ２２０２）、含まれている場合には、ＵＩＤ５０５を記憶装置２０５に保存する（ステップ２２０３）。

【０１４８】最後に、消費者２００は、受信した不可逆変換値$H_m$を記憶装置２０５に保存する（ステップ２２０４）。

【０１４９】なお、消費者２００は、受信した不可逆変換値$H_m$を記憶装置２０５に保存した回数をカウントすることで、何枚目のチケットが発券されたかを認識することができる。そこで、消費者端末２０１において、何枚目のチケットが発券されたかを示す表示が表示装置２０３になされるようにすることが好ましい。

【０１５０】図２２は、図１８のチケット発券要求処理（Ｓ２３００）の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム２０７ｃによって実現される。

【０１５１】図２２に示すように、チケット発券要求処理（Ｓ２３００）において、消費者２００は、まず、販売者１００に対して、販売者１００の公開鍵を要求し、公開鍵を受信する（ステップ２３０１）。

【０１５２】続いて、消費者２００は、自身だけしか知らないパスワード（初期チケット発券要求処理（Ｓ２１００）で入力したパスワードと同一のパスワード）を入力する（ステップ２３０２）。

【０１５３】続いて、消費者２００は、ステップ２３０２で入力したパスワードを、ステップ２３０１で入手した公開鍵を用いて暗号化し（ステップ２３０３）、暗号化したパスワード５０１と、図２１に示したチケット受信処理（Ｓ２２００）で入手したＵＩＤ５０５と、１回前のチケット受信処理（Ｓ２２００）で入手した不可逆変換値$H_m$とを、販売者１００に対して送信する（ステップ２３０４）。

【０１５４】このように、１回前のチケット受信処理（Ｓ２２００）で入手した不可逆変換値$H_m$を送信することによって、販売者１００は、消費者２００に発券した最新のチケットが何枚目であるか、すなわち、消費者２００が何枚目までのチケットを集めているかを知ることができるようになる。

【０１５５】なお、消費者２００は、１枚目のチケットの発券を要求すべきであるか（図１９に示した初期チケット発券要求処理（Ｓ２１００）を行うべきであるか）、または、２枚目以降のチケットの発券を要求すべきであるか（図２２に示したチケット発券要求処理（Ｓ

２３００）を行うべきであるか）については、記憶装置２０５にＵＩＤ５０５が記憶されているか否かで判断することができる。

【０１５６】図２３は、図１８のチケット発券処理（Ｓ１２００）の処理フローチャートであり、本処理は、チケット発券・検証処理プログラム１０７ｃによって実現される。

【０１５７】図２３に示すように、チケット発券処理（Ｓ１２００）において、販売者１００は、まず、暗号化されたパスワード５０１，ＵＩＤ５０５，不可逆変換値$H_m$を受信すると（ステップ１２０１）、受信したパスワード５０１を、販売者１００の秘密鍵を用いて復号する（ステップ１２０２）。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網３００を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【０１５８】続いて、販売者１００は、ステップ１２０２で復号したパスワード，ステップ１２０１で受信したＵＩＤ５０５，販売者１００の秘密鍵を結合したものの、不可逆変換値$H_1$を計算する（ステップ１２０３）。

【０１５９】続いて、販売者１００は、ステップ１２０１で受信した$H_m$とステップ１２０３で計算した$H_1$とが一致するか否かを検証し（ステップ１２０４）、一致した場合は、消費者２００がｎ枚のチケットを集め終えたことを意味しているので、ステップ１２０８に進んで、チケット収集完了処理を行う。なお、ステップ１２０８のチケット収集完了処理は、図１８のチケット収集終了処理（Ｓ１２５０）に相当しており、その処理内容は、販売者１００の販売方針に応じた様々な処理内容が考えられ、特に定めるものではない。

【０１６０】また、販売者１００は、ステップ１２０１で受信した$H_m$とステップ１２０３で計算した$H_1$とが一致しない場合は（ステップ１２０４）、消費者２００がｎ枚のチケットを集め終えていないことを意味しているので、$H_i$の不可逆変換値$H_{i+1}$（$1 \leqq i < n$）を計算し（ステップ１２０５）、$H_m = H_i$となるｉ（$1 < i \leqq n$）を求める（ステップ１２０６）。なお、ステップ１２０６では、販売者１００は、図２０に示した初期チケット発券処理（Ｓ１１００）のステップ１１０５と同様にして、$H_i$の不可逆変換値$H_{i+1}$（$1 \leqq i < n$）を繰り返し計算するが、$H_m = H_i$となるｉ（$1 < i \leqq n$）が求まった時点で、計算を中止することができる。

【０１６１】ここで、$H_m = H_i$となるｉが存在しない場合は、ステップ１２０１で受信したパスワード５０１，ＵＩＤ５０５，Ｈｍの少なくともいずれかが不正であることを意味しているので、エラー処理を実行する（ステップ１２０９）。

【０１６２】また、販売者１００は、$H_m = H_i$となるｉが存在する場合は、ＵＩＤ５０５と共に、$H_{i-1}$を、消費者２００に対して送信する（ステップ１２０７）。

【０１６３】以上説明したように、第２の実施形態に係る電子クーポンシステムにおいては、チケットの発券時に、販売者１００だけしか知らない秘密の情報である販売者１００の秘密鍵，消費者２００だけしか知らない情報であるパスワード，ｎ枚のチケットの組を識別するためのＵＩＤを連結したものから、不可逆変換値を繰り返し計算し、ｎ番目の不可逆変換値$H_n$，ｎ－１番目の不可逆変換値$H_{n-1}$，…，２番目の不可逆変換値$H_2$，１番目の不可逆変換値$H_1$という順番で、各不可逆変換値を消費者２００に対して返信するようにしている。また、消費者２００から販売者１００に対して、１回前に送信された$H_m$，ＵＩＤ，パスワードを送信するようにしている。また、不可逆変換値を計算するのに必要な消費者２００ごとのデータは、消費者２００から販売者１００に対して送信されるようにしている。

【０１６４】従って、第２の実施形態に係る電子クーポンシステムによれば、上述した第１の実施形態による効果に加えて、たとえチケットが通信路上で盗まれたとしても、パスワードを知らない第三者がチケットを不正使用するのを防止することができると共に、販売者１００側で、消費者２００ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【０１６５】なお、第２の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【０１６６】例えば、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００は、チケット発券時に、販売者１００の秘密鍵を用いて不可逆変換値を計算するようにしているが、この計算は、販売者１００以外が計算不可能であればよいので、不可逆変換のアルゴリズムが非公開であれば、販売者１００の秘密鍵を用いなくてもよい。

【０１６７】また、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００が、初期チケット発券時に、消費者２００に対してＵＩＤを送信し、消費者２００が、そのＵＩＤを保管しておき、その後は、保管しておいたＵＩＤを消費者２００から販売者１００に対して送信するようにしているが、チケット発券時に、その都度、販売者１００から消費者２００に対してＵＩＤを送信するようにしてもよい。

【０１６８】また、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００は、チケット発券時に、販売者１００の秘密鍵，パスワード，ＵＩＤを連結したものから計算した不可逆変換値を、消費者２００に対して返信するようにしているが、パスワードおよびＵＩＤを連結したものを、販売者１００だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における販売者１００の秘密鍵）を用いて暗号化し、暗号化した暗号化

情報を、消費者２００に対して返信するようにしてもよい。詳しくは、販売者１００は、パスワードおよびＵＩＤを連結したものの暗号化情報$H_1$に基づいて、暗号化情報$H_i$（$1 \leqq i < n$）の暗号化情報$H_{i+1}$を順次計算し、ｎ番目の暗号化情報$H_n$，ｎ－１番目の暗号化情報$H_{n-1}$，…，２番目の暗号化情報$H_2$，１番目の暗号化情報$H_1$という順番で、各暗号化情報を消費者２００に対して返信するようにしてもよい。

【０１６９】また、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００は、チケット発券時に、販売者１００の秘密鍵，パスワード，ＵＩＤを連結したものから計算した不可逆変換値を、消費者２００に対して返信するようにしているが、パスワード，ＵＩＤ，何枚目のチケットであるかを示す枚数情報を連結したものを、販売者１００だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における販売者１００の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者２００に対して返信するようにしてもよい。このようにすれば、販売者１００は、消費者２００からチケットの発券要求時に送信されてくる暗号化情報を、販売者１００だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報によって、消費者２００が何枚のチケットを集めたかを知ることができる。

【０１７０】また、第２の実施形態に係る電子クーポンシステムにおいては、販売者１００は、チケット発券時に、不可逆変換値を消費者２００に対して送信するようにしているが、上述した第１の実施形態で説明したクーポンと同様に、不可逆変換値を目視可能なデータとして記載したチケットを作成し、書面としてのチケットを消費者２００に対して送信するようにしてもよい。このようにすれば、消費者端末２０１においては、例えば、図２５に示すような表示が表示装置２０３になされて、何枚目のチケットが発券されたかを示すようにすることができる。

【０１７１】さらに、第２の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態で説明したクーポンと同様に、販売者１００から消費者２００に対して、チケットと共に、チケット全体のデジタル署名が送信されるようにしてもよく、このようにすれば、チケットの発券を受けた消費者２００側で、受け取ったチケットが改ざんされていないか否かを検証することができる。

【０１７２】（第３の実施形態）ところで、クーポンの発券を、販売者１００とは別に設けた専用の発券者が行うようにしてもよく、以下、クーポンの発券者を設けるようにした場合を、第３の実施形態として、上述した第１の実施形態と異なる点についてのみ説明する。

【０１７３】図２６は、第３の実施形態に係る電子クーポンシステムの概略構成を示す図である。

【０１７４】第３の実施形態に係る電子クーポンシステムは、消費者$200_1$～$200_n$（以下、単に「消費者２００」とも称す。），販売者端末$600_1$～$600_n$（以下、単に「販売者６００」とも称す。），発券者７００が利用するシステムであり、図２６に示すように、消費者２００が利用する端末である消費者端末$201_1$～$201_n$（以下、単に「消費者端末２０１」とも称す。）と、販売者６００が利用する端末である販売者端末$601_1$～$601_n$（以下、単に「販売者端末６０１」とも称す。）と、発券者７００が利用する端末である発券者端末７０１とが、インターネット等の通信網３００を介して互いに接続されて構成されている。

【０１７５】次に、第３の実施形態に係る電子クーポンシステムを構成する発券者端末７０１および販売店端末６０１のハードウェア構成について、図２７および図２８を用いて説明する。なお、消費者端末２０１のハードウェア構成は、図３に示したハードウェア構成と同様である。

【０１７６】図２７は発券者端末７０１のハードウェア構成を示す図である。

【０１７７】図２７に示すように、発券者端末７０１は、通信インタフェース７０２と、表示装置７０３と、入力装置７０４と、記憶装置７０５と、中央処理装置（ＣＰＵ）７０６と、一時記憶装置（メモリ）７０７とが、バス７１０によって互いに接続された構成となっており、基本的には、図２に示した販売者端末１０１のハードウェア構成と同様である。

【０１７８】メモリ７０７には、ＯＳ７０７ａや、クーポン発券・検証処理プログラム７０７ｂといった、ＣＰＵ７０６が実行するプログラム等が一時的に格納される。

【０１７９】ここで、ＯＳ７０７ａは、発券者端末７０１全体の制御を行うために、ファイル管理，プロセス管理，デバイス管理といった機能を実現するためのプログラムである。また、クーポン発券・検証処理プログラム７０７ｂは、消費者２００に対してクーポンを発券したり、販売者６００から検証（後述するように、クーポンの二重使用についての検証である。）が要求されたクーポンを検証したりするためのプログラムである。

【０１８０】図２８は販売者端末６０１のハードウェア構成を示す図である。

【０１８１】図２に示したハードウェア構成と異なる点は、メモリ１０７に、クーポン発券・検証処理プログラム１０７ｂの代わりに、クーポン検証処理プログラム６０７ｂが一時的に格納される点である。

【０１８２】クーポン検証処理プログラム６０７ｂは、消費者２００から使用が要求されたクーポンを検証するためのプログラムである。

【０１８３】次に、第３の実施形態に係る電子クーポンシステムの動作について説明する。

【０１８４】なお、以下の説明おいても、上述した第１

の実施形態と同様に、消費者２００が行う処理は、実際には、消費者２００の指示によって消費者端末２０１が実行し、販売者６００が行う処理は、実際には、販売者６００の指示によって販売者端末６０１が実行するものであり、さらに、発券者７００が行う処理は、実際には、発券者７００の指示によって発券者端末７０１が実行するものである。

【０１８５】図２９は、消費者２００が、発券者７００に対してクーポンの発券を要求し、発券者７００によって発券されたクーポンを受信するまでの動作を説明するための図である。

【０１８６】図２９において、まず、消費者２００は、発券者７００からクーポンの発券を受ける条件を満たしているものとする（Ｓ２０００）。

【０１８７】消費者２００は、後述するクーポン要求処理（Ｓ１２４００）を行い、暗号化した自身のパスワード５０１を、発券者７００に対して送信する。

【０１８８】発券者７００は、パスワード５０１を受信すると、後述するクーポン発券処理（Ｓ７３００）を行い、クーポン５０２と、クーポン５０２のデジタル署名５０３とを、消費者２００に対して送信する。

【０１８９】消費者２００は、クーポン５０２およびデジタル署名５０３を受信すると、後述するクーポン受信処理（Ｓ１２５００）を行い、受信したクーポン５０２を保管する。

【０１９０】図２９に示した動作は、図４に示した動作において、販売者１００が発券者７００に代わっている点が異なる。

【０１９１】すなわち、図２９のクーポン要求処理（Ｓ１２４００）の処理フローチャートは、図７に示したクーポン要求処理（Ｓ２４００）の処理フローチャートと同様であるが、販売者１００の公開鍵の代わりに発券者７００の公開鍵を用いる点と、暗号化したパスワード５０１の送信先が、販売者１００の代わりに発券者７００となる点とが異なる。

【０１９２】また、図２９のクーポン発券処理（Ｓ７３００）の処理フローチャートは、図８に示したクーポン発券処理（Ｓ１３００）の処理フローチャートと同様であるが、本処理を発券者７００が行う点（本処理がクーポン発券・検証処理プログラム７０７ｂによって実現される点）と、販売者１００の秘密鍵の代わりに発券者７００の秘密鍵を用いる点とが異なる。

【０１９３】また、図２９のクーポン受信処理（Ｓ１２５００）の処理フローチャートは、図９に示したクーポン受信処理（Ｓ２５００）の処理フローチャートと同様である。

【０１９４】図３０は、既にクーポンの発券を受けている消費者２００が、通信網３００を介してクーポンを使用し、販売者６００が、クーポンを検証するまでの動作を説明するための図である。

【０１９５】図３０において、既にクーポンの発券を受けている消費者２００は、クーポン使用オンライン処理（Ｓ２６００）を行い、クーポン受信処理（Ｓ１２５００）で入手したクーポン５０２と、暗号化した自身のパスワード５０１とを、販売者６００に対して送信する。

【０１９６】販売者６００は、クーポン５０２およびパスワード５０１を受信すると、後述するクーポン検証処理（Ｓ６４００）を行い、受信したクーポン５０２を検証する。

【０１９７】図３１は、既にクーポンの発券を受けている消費者２００が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者６００が、クーポンを検証するまでの動作を説明するための図である。

【０１９８】図３１において、既にクーポンの発券を受けている消費者２００は、クーポン使用オフライン処理（Ｓ２７００）を行い、印刷されたクーポン５０４を販売店に持参する。

【０１９９】販売者６００は、消費者２００が持参したクーポン５０４を受け取ると、後述するクーポン検証処理（Ｓ６４００）を行い、受け取ったクーポン５０４を検証する。

【０２００】図３０および図３１に示した動作は、各々、図５および図６に示した動作において、販売者６００が行うクーポン検証処理（Ｓ６４００）の処理内容のみが異なり、本処理の処理内容については後述する。

【０２０１】すなわち、図３０のクーポン使用オンライン処理（Ｓ２６００）の処理フローチャートは、図１０に示したクーポン使用オンライン処理（Ｓ２６００）の処理フローチャートと同様である。

【０２０２】また、図３１のクーポン使用オフライン処理（Ｓ２７００）の処理フローチャートは、図１１に示したクーポン使用オフライン処理（Ｓ２７００）の処理フローチャートと同様である。

【０２０３】図３２は、図３０および図３１のクーポン検証処理（Ｓ６４００）の処理フローチャートであり、本処理は、クーポン検証処理プログラム６０７ｂによって実現される。

【０２０４】図３２に示すように、クーポン検証処理（Ｓ６４００）においては、販売者６００は、図１２に示したクーポン検証処理（Ｓ１２００）と同様の処理を行うが、ステップ１１４０４の書面検証処理の処理内容が、後述するように異なる。

【０２０５】また、販売者６００は、使用済みシリアル番号リストを管理せず、ステップ１１４０６で、クーポンに記載されているシリアル番号を発券者７００に対して通知し、使用済みシリアル番号リストへのシリアル番号の登録を発券者７００に行ってもらうようにしている点が異なる。

【０２０６】図３３は、図３２の書面検証処理（ステップ１１４０４）の処理フローチャートである。

【０２０７】図３３に示すように、書面検証処理（ステップ１１４０４）においては、販売者６００は、図１３に示した書面検証処理と同様の処理を行うが、ステップ１１４１０で、クーポンに記載されているデジタル署名を、発券者７００の公開鍵を用いて復号している点と、ステップ１１４１４で、クーポンに記載されているシリアル番号を発券者７００に対して通知し、使用済みシリアル番号リストにシリアル番号が登録されているか否かを発券者７００に問い合わせるようにしている点とが異なる。そこで、販売者６００は、ステップ１４１１の検証では、ステップ１１４１０で復号した結果と、クーポンに記載されているクーポン情報とを比較することとなる。

【０２０８】以上説明したように、第３の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態と同様に、シリアル番号，有効期限，金額等の改ざんされては困るクーポン情報のデジタル署名を、発券者７００だけしか知らない情報である秘密鍵を用いて計算し、計算したデジタル署名を、目視可能なデータとして記載したクーポンを作成するようにしている。

【０２０９】従って、第３の実施形態に係る電子クーポンシステムによれば、上述した第１の実施形態と同様に、消費者２００が電子的なクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されているデジタル署名を検証することで、クーポンの偽造や改ざんを検出することができる。

【０２１０】なお、第３の実施形態に係る電子クーポンシステムでは、デジタル署名を作成する発券者７００と、デジタル署名を検証する販売者６００とが異なるが、デジタル署名の作成時に発券者７００の秘密鍵を用い、デジタル署名の検証時に発券者７００の公開鍵を用いるようにすることで、販売者６００によるデジタル署名の検証が可能である。ただし、販売者６００および発券者７００の双方だけしか知らない秘密の暗号鍵を用いて、クーポン情報を暗号化し、暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにしても、販売者６００による暗号化情報の検証は可能である。

【０２１１】また、第３の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態と同様に、クーポンの発券時に、消費者２００が提示したパスワードの不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしている。さらに、クーポンの使用時には、発券を要求した消費者２００だけしか知らないパスワードを販売者６００に提示し、消費者２００が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較するようにしている。

【０２１２】従って、第３の実施形態に係る電子クーポンシステムによれば、上述した第１の実施形態と同様に、たとえクーポンが盗まれたとしても、クーポンの発券要求時に提示されたパスワードを知らない第三者がクーポンを不正使用するのを防止することができる。

【０２１３】なお、第３の実施形態に係る電子クーポンシステムにおいては、パスワードについて、不可逆変換を施した不可逆変換値を、目視可能なデータとしてクーポンに記載するようにした例を示しており、本例によれば、不可逆変換方法を公開しても支障がないので、販売者６００による不可逆変換値の検証が可能であると共に、パスワードの不可逆変換値が不一致である場合に、消費者２００が、自身が提示したパスワードの不可逆変換値を計算して確認することが可能である。しかしながら、パスワードについて、販売者６００および発券者７００の双方だけしか暗号化できない暗号化方法で暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにしても、販売者６００による暗号化情報の検証は可能である。

【０２１４】なお、第３の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【０２１５】例えば、第３の実施形態に係る電子クーポンシステムにおいては、消費者２００は、発券者７００および販売者６００に対してパスワードを送信するときに、発券者７００および販売者６００の公開鍵を取得し、暗号通信を行うようにしているが、本発明はこれに限定しない。消費者２００は、１度、発券者７００および販売者６００の公開鍵を入手すれば、２回以降は、その公開鍵を使うことができる。また、発券者７００および販売者６００と消費者２００との間で共通の鍵を持つことができれば、秘密鍵暗号技術を使って暗号化するようにしてもよい。

【０２１６】また、第３の実施形態に係る電子クーポンシステムにおいて、消費者２００から発券者７００および販売者６００に対してパスワードを送信するときに、暗号化されたパスワードがそのまま盗まれて不正使用されるのを防止するために、パスワードを、その他の情報（乱数や適当な数字でよい。）と共に暗号化して送信するようにしてもよい。

【０２１７】また、第３の実施形態に係る電子クーポンシステムにおいては、発券者７００は、デジタル署名を、数値や文字等の目視可能なデータとしてクーポンに記載するようにしているが、印刷後に目視可能であれば、例えば、バーコード等のようなものであってもよい。バーコードとして記載すれば、販売者６００は、印刷されたクーポンから各種情報を取得する際に、バーコードリーダを用いることができるようになる。

【０２１８】また、第３の実施形態に係る電子クーポンシステムにおいては、発券者７００は、消費者２００のパスワードの不可逆変換値と、シリアル番号，有効期

限，金額等のクーポン情報のデジタル署名とを、別々にクーポンに記載するようにしているが、クーポン情報と共に、パスワードも一緒にデジタル署名を計算するようにしてもよい。また、このとき、クーポン情報やパスワード等の、デジタル署名を計算する元の情報は、不可逆変換を施した後に、デジタル署名を計算するようにしてもよい。

【０２１９】また、第３の実施形態に係る電子クーポンシステムにおいては、消費者２００から使用が要求されたクーポンを販売者６００が検証し、クーポンの二重使用のみを発券者７００が一元管理して検証する方法を取っているが、販売者６００が受け取ったクーポンを、そのときに提示されたパスワードと共に発券者７００に提示し、発券者７００側でクーポンを検証するようにしてもよい。また、その両方を組み合わせるようにしてもよい。

【０２２０】発券者７００側でクーポンを検証するようにすれば、発券者７００だけしか知らない秘密の暗号鍵を用いてクーポン情報を暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにすることができる。また、発券者７００だけしか暗号化できない暗号化方法でパスワードを暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにすることもできる。

【０２２１】（第４の実施形態）ところで、上述した第３の実施形態に係る電子クーポンシステムにおいて、発券者７００は、上述した第２の実施形態で説明したように、チケットを取り扱うようにすることができ、そのようにした場合を、第４の実施形態として、上述した第２の実施形態および第３の実施形態と異なる点についてのみ説明する。

【０２２２】第４の実施形態に係る電子クーポンシステムの概略構成は、図２６に示した概略構成と同様である。

【０２２３】図３４は発券者端末７０１のハードウェア構成を示す図である。

【０２２４】図２７に示したハードウェア構成と異なる点は、メモリ７０７に、チケット発券・検証処理プログラム７０７ｃが一時的に格納される点である。

【０２２５】チケット発券・検証処理プログラム７０７ｃは、消費者２００に対してチケットを発券したり、消費者２００から使用が要求されたチケットを検証したりするためのプログラムである。

【０２２６】なお、販売者端末６０１のハードウェア構成は、図２８に示したハードウェア構成と同様であり、消費者端末２０１のハードウェア構成は、図１６に示したハードウェア構成と同様である。

【０２２７】次に、第４の実施形態に係る電子クーポンシステムの動作について説明する。

【０２２８】なお、以下の説明おいても、上述した第３の実施形態と同様に、消費者２００が行う処理は、実際には、消費者２００の指示によって消費者端末２０１が実行し、発券者７００が行う処理は、実際には、発券者７００の指示によって発券者端末７０１が実行するものである。

【０２２９】図３５は、消費者２００が、発券者７００に対して１枚目のチケットの発券を要求し、発券者７００によって発券された１枚目のチケットを受信するまでの動作を説明するための図である。なお、チケットは、ｎ枚だけ集めたときに効力を発揮するものとする。

【０２３０】図３５において、まず、消費者２００は、後述する初期チケット発券要求処理（Ｓ１２１００）を行い、暗号化した自身のパスワード５０１を、発券者７００に対して送信する。

【０２３１】発券者７００は、パスワード５０１を受信すると、後述する初期チケット発券処理（Ｓ７１００）を行い、ｎ枚のチケットの組を識別するために付与した固有の値（以下、「ＵＩＤ」と称す。）５０５と、受信したパスワード５０１，ＵＩＤ５０５，発券者７００だけしか知らない秘密の情報（例えば、発券者７００の秘密鍵）を連結したものの、ｎ番目の不可逆変換値$H_n(506_n)$とを、１枚目のチケットとして、消費者２００に対して送信する。

【０２３２】消費者２００は、ＵＩＤ５０５および$H_n(506_n)$を受信すると、後述するチケット受信処理（Ｓ１２２００）を行い、受信したＵＩＤ５０５および$H_n(506_n)$を保管する。

【０２３３】図３５に示した動作は、図１７に示した動作において、販売者１００が発券者７００に代わっている点が異なる。

【０２３４】すなわち、図３５の初期チケット発券要求処理（Ｓ１２１００）の処理フローチャートは、図１９に示した初期チケット発券要求処理（Ｓ２１００）の処理フローチャートと同様であるが、販売者１００の公開鍵の代わりに発券者７００の公開鍵を用いる点と、暗号化したパスワード５０１の送信先が、販売者１００の代わりに発券者７００となる点とが異なる。

【０２３５】また、図３５の初期チケット発券処理（Ｓ７１００）の処理フローチャートは、図２０に示した初期チケット発券処理（Ｓ１１００）の処理フローチャートと同様であるが、本処理を発券者７００が行う点（本処理がチケット発券・検証処理プログラム７０７ｃによって実現される点）と、販売者１００の秘密鍵の代わりに発券者７００の秘密鍵を用いる点とが異なる。

【０２３６】また、図３５のチケット受信処理（Ｓ１２２００）の処理フローチャートは、図２１に示したチケット受信処理（Ｓ２２００）の処理フローチャートと同様である。

【０２３７】図３６は、消費者２００が、発券者７００

に対して２枚目以降のチケットの発券を要求し、発券者７００によって発券された２枚目以降のチケットを受信するまでの動作を説明するための図である。

【０２３８】図３６において、まず、消費者２００は、２枚目のチケットの発券を受ける場合は、後述するチケット発券要求処理（Ｓ１２３００）を行い、暗号化した自身のパスワード５０１と、１枚目のチケット受信処理（Ｓ１２２００）で入手したＵＩＤ５０５および$H_n(506_n)$とを、発券者７００に対して送信する。

【０２３９】発券者７００は、パスワード５０１，ＵＩＤ５０５，$H_n(506_n)$を受信すると、後述するチケット発券処理（Ｓ７２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，$H_n(506_n)$と、発券者７００の秘密鍵とから、$H_{n-1}(506_{n-1})$を求めて、求めた$H_{n-1}(506_{n-1})$を、２枚目のチケットとして、消費者２００に対して送信する。

【０２４０】消費者２００は、$H_{n-1}(506_{n-1})$を受信すると、チケット受信処理（Ｓ１２２２００）を行い、受信した$H_{n-1}(506_{n-1})$を保管する。

【０２４１】同様に、消費者２００は、ｍ＋１枚目（１≦ｍ＜ｎ）のチケットの発券を受ける場合は、チケット発券要求処理（Ｓ１２３００）を行い、暗号化した自身のパスワード５０１と、ｍ枚目のチケット受信処理（Ｓ１２２００）で入手したＵＩＤ５０５および$H_{n-(m-1)}(506_{n-(m-1)})$とを、発券者７００に対して送信する。

【０２４２】発券者７００は、パスワード５０１，ＵＩＤ５０５，$H_{n-(m-1)}(506_{n-(m-1)})$を受信すると、チケット発券処理（Ｓ７２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，$H_{n-(m-1)}(506_{n-(m-1)})$と、発券者７００の秘密鍵とから、$H_{n-m}(506_{n-m})$を求めて、求めた$H_{n-m}(506_{n-m})$を、ｍ＋１枚目のチケットとして、消費者２００に対して送信する。

【０２４３】消費者２００は、$H_{n-m}(506_{n-m})$を受信すると、チケット受信処理（Ｓ１２２２００）を行い、受信した$H_{n-m}(506_{n-m})$を保管する。

【０２４４】このようにして、消費者２００は、ｎ枚のチケットを集めることができ、これらｎ枚のチケットの効力を発揮させたい場合には、チケット発券要求処理（Ｓ１２３００）を行い、暗号化された自身のパスワード５０１と、ｎ枚目のチケット受信処理（Ｓ１２２００）で入手したＵＩＤ５０５および$H_1(506_1)$とを、発券者７００に対して送信する。

【０２４５】発券者７００は、パスワード５０１，ＵＩＤ５０５，$H_1(506_1)$を受信すると、チケット発券処理（Ｓ７２００）を行い、受信したパスワード５０１，ＵＩＤ５０５，$H_1(506_1)$と、発券者７００の秘密鍵とから、消費者２００がｎ枚だけチケットを集めたことを確認し、ｎ枚のチケット収集終了処理（Ｓ７２５０）を行う。

【０２４６】図３６に示した動作は、図１８に示した動作において、販売者１００が発券者７００に代わっている点が異なる。

【０２４７】すなわち、図３６のチケット発券要求処理（Ｓ１２１００）の処理フローチャートは、図２２に示したチケット発券要求処理（Ｓ２３００）の処理フローチャートと同様であるが、販売者１００の公開鍵の代わりに発券者７００の公開鍵を用いる点と、暗号化したパスワード５０１，保存しているＵＩＤ５０５および$H_m$の送信先が、販売者１００の代わりに発券者７００となる点とが異なる。

【０２４８】また、図３６のチケット発券処理（Ｓ７１００）の処理フローチャートは、図２３に示したチケット発券処理（Ｓ１２００）の処理フローチャートと同様であるが、本処理を発券者７００が行う点（本処理がチケット発券・検証処理プログラム７０７ｃによって実現される点）と、販売者１００の秘密鍵の代わりに発券者７００の秘密鍵を用いる点とが異なる。

【０２４９】また、図３６のチケット受信処理（Ｓ１２２００）の処理フローチャートは、図２１に示したチケット受信処理（Ｓ２２００）の処理フローチャートと同様である。

【０２５０】なお、チケットをｎ枚だけ集めたときに発揮する効力は、販売者１００の販売方針に応じて異なるようにすることができるが、チケットをｎ枚だけ集めたか否かの判定を、発券者７００が行うようにしているので、図３６のチケット収集終了処理（Ｓ７２５０）は、発券者７００が行うものとしている。

【０２５１】以上説明したように、第４の実施形態に係る電子クーポンシステムにおいても、上述した第２の実施形態と同様に、チケットの発券時に、発券者７００だけしか知らない秘密の情報である発券者７００の秘密鍵，消費者２００だけしか知らない情報であるパスワード，ｎ枚のチケットの組を識別するためのＵＩＤを連結したものから、不可逆変換値を繰り返し計算し、ｎ番目の不可逆変換値$H_n$，ｎ－１番目の不可逆変換値$H_{n-1}$，…，２番目の不可逆変換値$H_2$，１番目の不可逆変換値$H_1$という順番で、各不可逆変換値を消費者２００に対して返信するようにしている。また、消費者２００から発券者７００に対して、１回前に送信された$H_m$，ＵＩＤ，パスワードを送信するようにしている。また、不可逆変換値を計算するのに必要な消費者２００ごとのデータは、消費者２００から発券者７００に対して送信されるようにしている。

【０２５２】従って、第４の実施形態に係る電子クーポンシステムによれば、上述した第３の実施形態による効果に加えて、上述した第２の実施形態と同様に、たとえチケットが通信路上で盗まれたとしても、パスワードを知らない第三者がチケットを不正使用するのを防止することができると共に、発券者７００側で、消費者２００

ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【０２５３】なお、第４の実施形態に係る電子クーポンシステムにおいても、上述した第３の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【０２５４】例えば、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００は、チケット発券時に、発券者７００の秘密鍵を用いて不可逆変換値を計算するようにしているが、この計算は、発券者７００以外が計算不可能であればよいので、不可逆変換のアルゴリズムが非公開であれば、発券者７００の秘密鍵を用いなくてもよい。

【０２５５】また、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００が、初期チケット発券時に、消費者２００に対してＵＩＤを送信し、消費者２００が、そのＵＩＤを保管しておき、その後は、保管しておいたＵＩＤを消費者２００から発券者７００に対して送信するようにしているが、チケット発券時に、その都度、発券者７００から消費者２００に対してＵＩＤを送信するようにしてもよい。

【０２５６】また、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００は、チケット発券時に、発券者７００の秘密鍵，パスワード，ＵＩＤを連結したものから計算した不可逆変換値を、消費者２００に対して返信するようにしているが、パスワードおよびＵＩＤを連結したものを、発券者７００だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における発券者７００の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者２００に対して返信するようにしてもよい。詳しくは、発券者７００は、パスワードおよびＵＩＤを連結したものの暗号化情報$H_1$に基づいて、暗号化情報$H_i$（$1 \leqq i < n$）の暗号化情報$H_{i+1}$を順次計算し、ｎ番目の暗号化情報$H_n$，ｎ－１番目の暗号化情報$H_{n-1}$，…，２番目の暗号化情報$H_2$，１番目の暗号化情報$H_1$という順番で、各暗号化情報を消費者２００に対して返信するようにしてもよい。

【０２５７】また、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００は、チケット発券時に、発券者７００の秘密鍵，パスワード，ＵＩＤを連結したものから計算した不可逆変換値を、消費者２００に対して返信するようにしているが、パスワード，ＵＩＤ，何枚目のチケットであるかを示す枚数情報を連結したものを、発券者７００だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における発券者７００の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者２００に対して返信するようにしてもよい。このようにすれば、発券者７００は、消費者２００からチケットの発券要求時に送信されてくる暗号化情報を、発券者７００だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報によって、消費者２００が何枚のチケットを集めたかを知ることができる。

【０２５８】また、第４の実施形態に係る電子クーポンシステムにおいては、発券者７００は、チケット発券時に、不可逆変換値を消費者２００に対して送信するようにしているが、上述した第１の実施形態で説明したクーポンと同様に、不可逆変換値を目視可能なデータとして記載したチケットを作成し、書面としてのチケットを消費者２００に対して送信するようにしてもよい。

【０２５９】さらに、第４の実施形態に係る電子クーポンシステムにおいても、上述した第１の実施形態で説明したクーポンと同様に、発券者７００から消費者２００に対して、チケットと共に、チケット全体のデジタル署名が送信されるようにしてもよく、このようにすれば、チケットの発券を受けた消費者２００側で、受け取ったチケットが改ざんされていないか否かを検証することができる。

【０２６０】

【発明の効果】以上説明したように、本発明によれば、電子的に発券されたクーポンが印刷されて使用される場合でも、クーポンの偽造や改ざん，第三者によるクーポンの不正使用を検出することができるようになるので、消費者は、電子的に発券されたクーポンを、ネットワーク上に開設されたバーチャル販売店だけではなく、現実に存在する販売店でも使用することができるようになる。

【０２６１】さらに、本発明によれば、複数枚だけ集めたときに効力を発揮するチケットを取り扱う場合に、チケットを発券する側で消費者を管理する必要がなくなるので、チケットを発券する側の手間を減らすことができるようになる。

【図面の簡単な説明】

【図１】第１の実施形態に係る電子クーポンシステムの概略構成図。

【図２】第１の実施形態における販売者端末のハードウェア構成図。

【図３】第１の実施形態における消費者端末のハードウェア構成図。

【図４】第１の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対してクーポンの発券を要求し、販売者によって発券されたクーポンを受信するまでの動作の説明図。

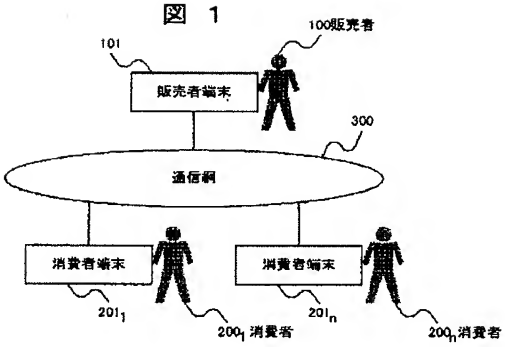
【図５】第１の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、通信網を介してクーポンを使用し、販売者が、クーポンを検証するまでの動作の説明図。

【図６】第１の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者が、クーポンを検証するまでの

動作の説明図。
【図７】図４のクーポン要求処理の処理フローチャート。
【図８】図４のクーポン発券処理の処理フローチャート。
【図９】図４のクーポン受信処理の処理フローチャート。
【図１０】図５のクーポン使用オンライン処理の処理フローチャート。
【図１１】図６のクーポン使用オフライン処理の処理フローチャート。
【図１２】図５および図６のクーポン検証処理の処理フローチャート。
【図１３】図１２のステップ１４０４で行われる書面検証処理の処理フローチャート。
【図１４】第１の実施形態に係る電子クーポンシステムで発券されるクーポンの形式の一例を示す説明図。
【図１５】第２の実施形態における販売者端末のハードウェア構成図。
【図１６】第２の実施形態における消費者端末のハードウェア構成図。
【図１７】第２の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対して１枚目のチケットの発券を要求し、販売者によって発券された１枚目のチケットを受信するまでの動作の説明図。
【図１８】第２の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対して２枚目以降のチケットの発券を要求し、販売者によって発券された２枚目以降のチケットを受信するまでの動作の説明図。
【図１９】図１７の初期チケット発券要求処理の処理フローチャート。
【図２０】図１７の初期チケット発券処理の処理フローチャート。
【図２１】図１７および図１８のチケット受信処理の処理フローチャート。
【図２２】図１８のチケット発券要求処理の処理フローチャート。
【図２３】図１８のチケット発券処理の処理フローチャート。
【図２４】図２０のステップ１１０５で不可逆変換値が計算される様子を示す説明図。
【図２５】第２の実施形態における消費者端末での表示の一例を示す説明図。
【図２６】第３の実施形態に係る電子クーポンシステムの概略構成図。
【図２７】第３の実施形態における発券者端末のハードウェア構成図。
【図２８】第３の実施形態における販売者端末のハードウェア構成図。
【図２９】第３の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対してクーポンの発券を要求し、発券者によって発券されたクーポンを受信するまでの動作の説明図。
【図３０】第３の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、通信網を介してクーポンを使用し、販売者が、クーポンを検証するまでの動作の説明図。
【図３１】第３の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者が、クーポンを検証するまでの動作の説明図。
【図３２】図３０および図３１のクーポン検証処理の処理フローチャート。
【図３３】図３２のステップ１１４０４で行われる書面検証処理の処理フローチャート。
【図３４】第４の実施形態における発券者端末のハードウェア構成図。
【図３５】第４の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対して１枚目のチケットの発券を要求し、発券者によって発券された１枚目のチケットを受信するまでの動作の説明図。
【図３６】第４の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対して２枚目以降のチケットの発券を要求し、発券者によって発券された２枚目以降のチケットを受信するまでの動作の説明図。
【符号の説明】
１００，６００…販売者、２００$_1$～２００$_n$…消費者、７００…発券者、１０１，６０１$_1$～６０１$_n$…販売者端末、２０１$_1$～２０１$_n$…消費者端末、７０１…発券者端末、３００…通信網、１０２，２０２，７０２…通信網インタフェース、１０３，２０３，７０３…表示装置、１０４，２０４，７０４…入力装置、１０５，２０５，７０５…記憶装置、１０６，２０６，７０６…中央処理装置（ＣＰＵ）、１０７，２０７，７０７…一時記憶装置（メモリ）、２０８…印刷装置、１１０，２１０，７１０…バス、１０７ａ，２０７ａ，７０７ａ…オペレーティングシステム（ＯＳ）、１０７ｂ，７０７ｂ…クーポン発券・検証処理プログラム、１０７ｃ，７０７ｃ…チケット発券・検証処理プログラム、２０７ｂ…クーポン要求・受信・発信処理プログラム、６０７ｂ…クーポン検証処理プログラム、２０７ｃ…チケット要求・受信・発信処理プログラム、５０１…パスワード、５０２…クーポン、５０３…デジタル署名、５０４…印刷されたクーポン、５０５…ＵＩＤ、５０６$_1$～５０６$_n$…不可逆変換値、５０７…秘密鍵。

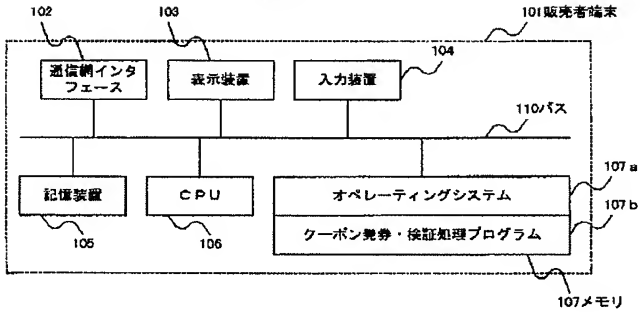
【図１】

図 1



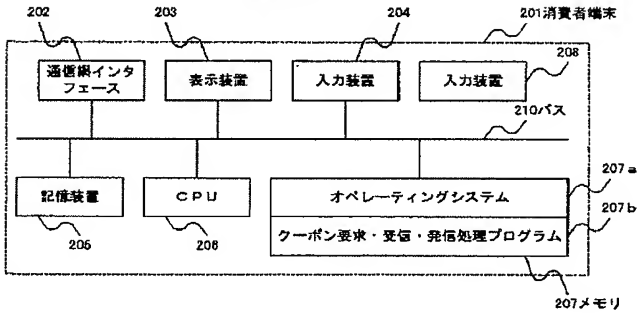

【図２】

図 2



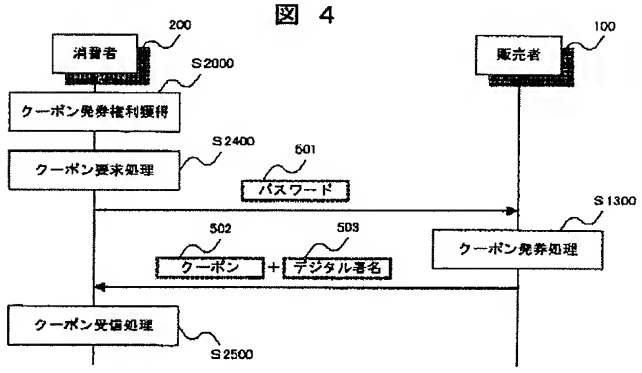

【図３】

図 3



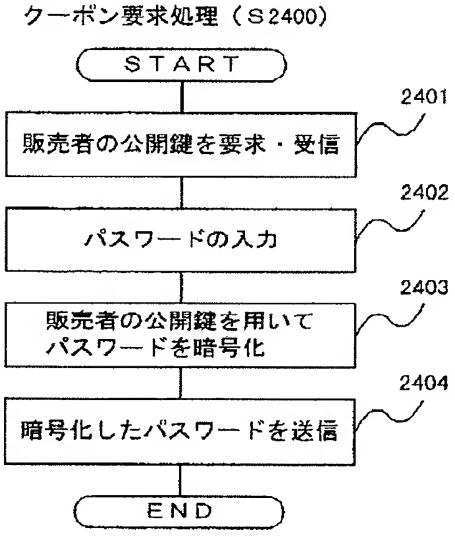

【図４】

図 4



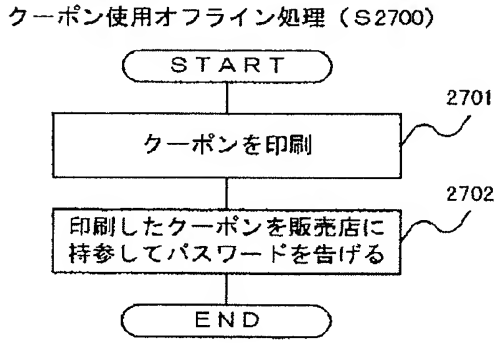

【図７】

図 7



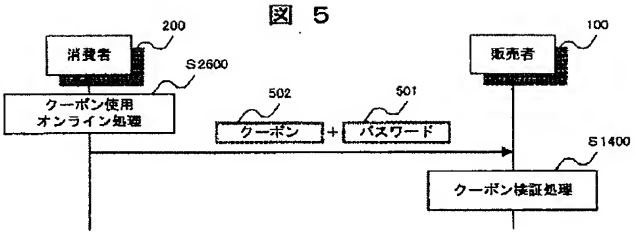

【図１１】

図 11



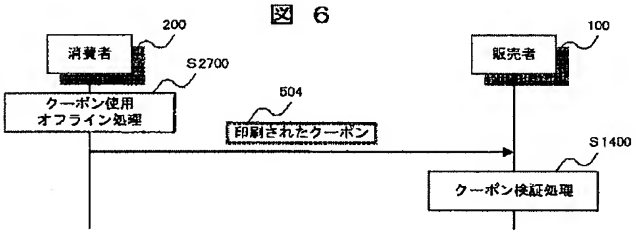
【図５】

図 5




【図６】

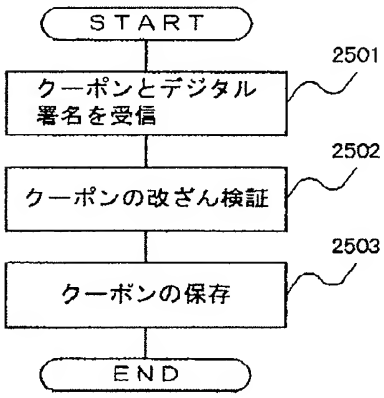
図 6




【図９】

図 9

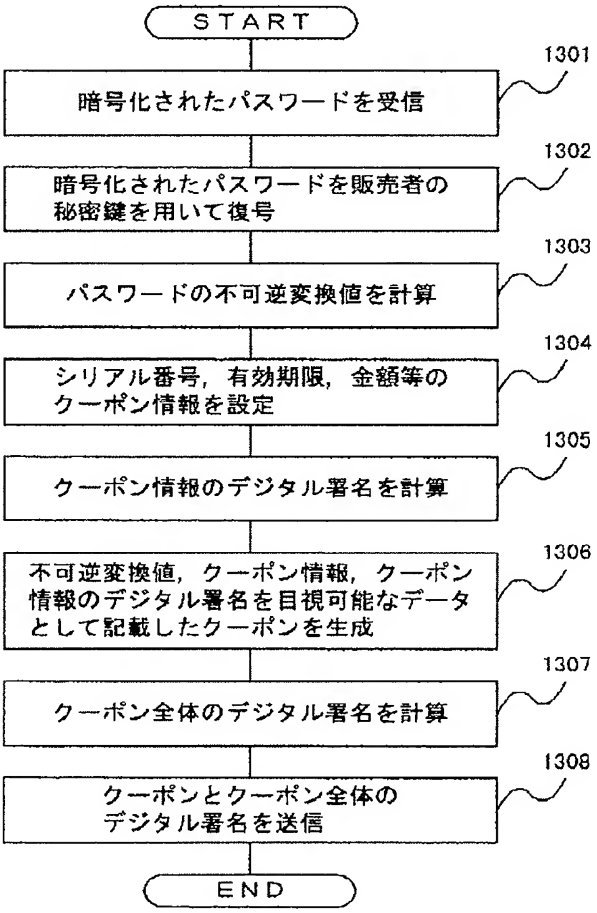
クーポン受信処理（S2500）




【図８】

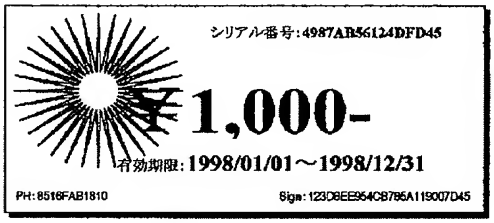
図 8

クーポン発券処理（S1300）




【図１４】

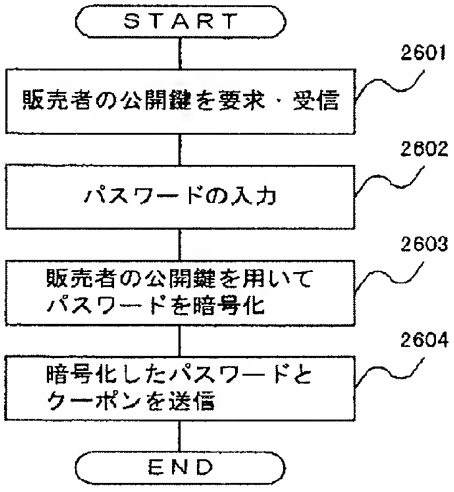
図 14



【図１０】

図 10

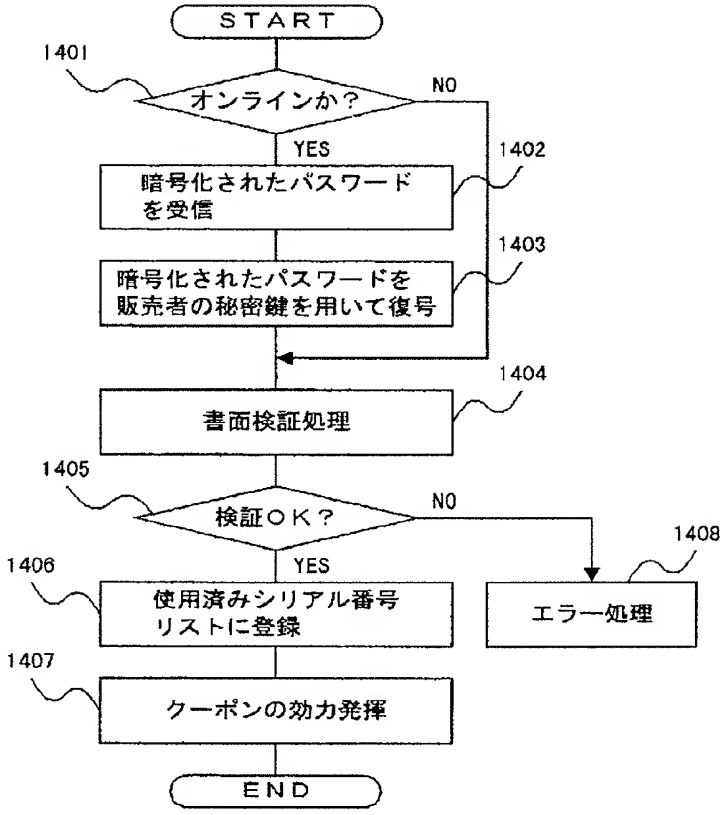
クーポン使用オンライン処理（Ｓ2600）




【図１２】

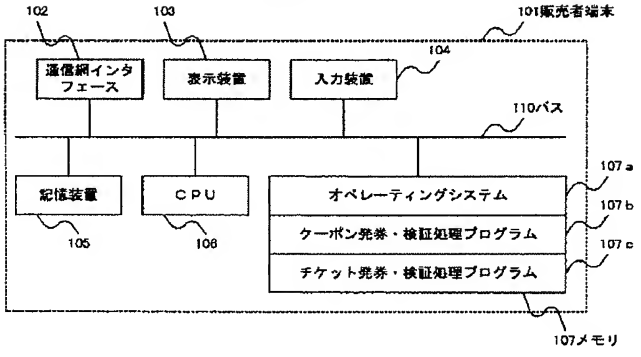
図 12

クーポン検証処理（Ｓ1400）



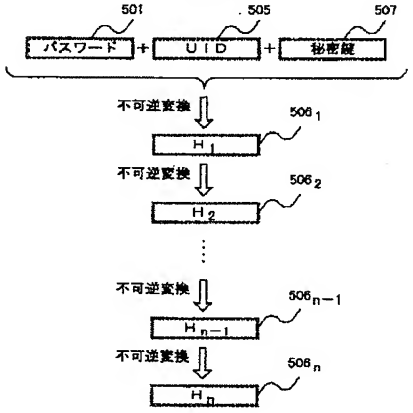

【図１５】

図 15



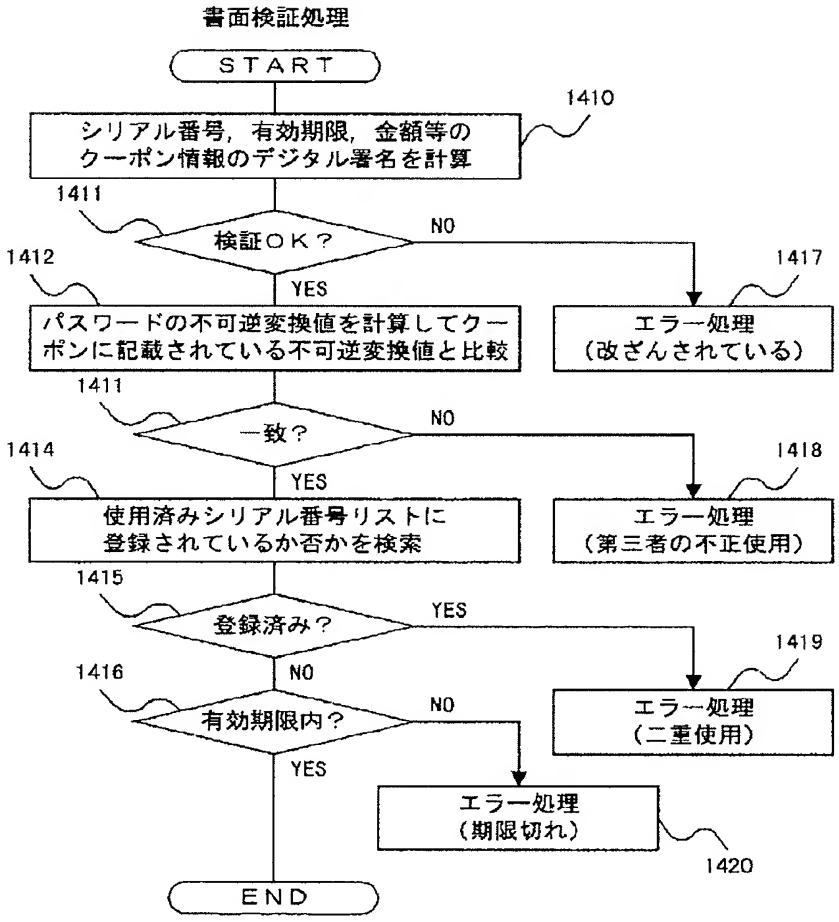

【図２４】

図 24



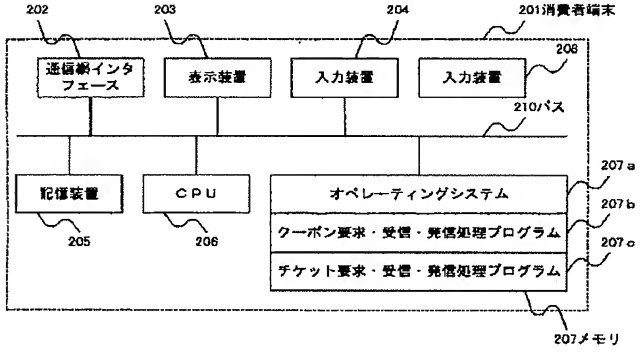
【図１３】

図 13



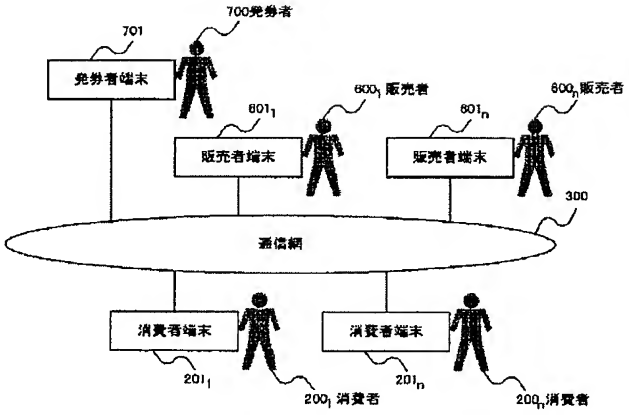

【図１６】

図 16



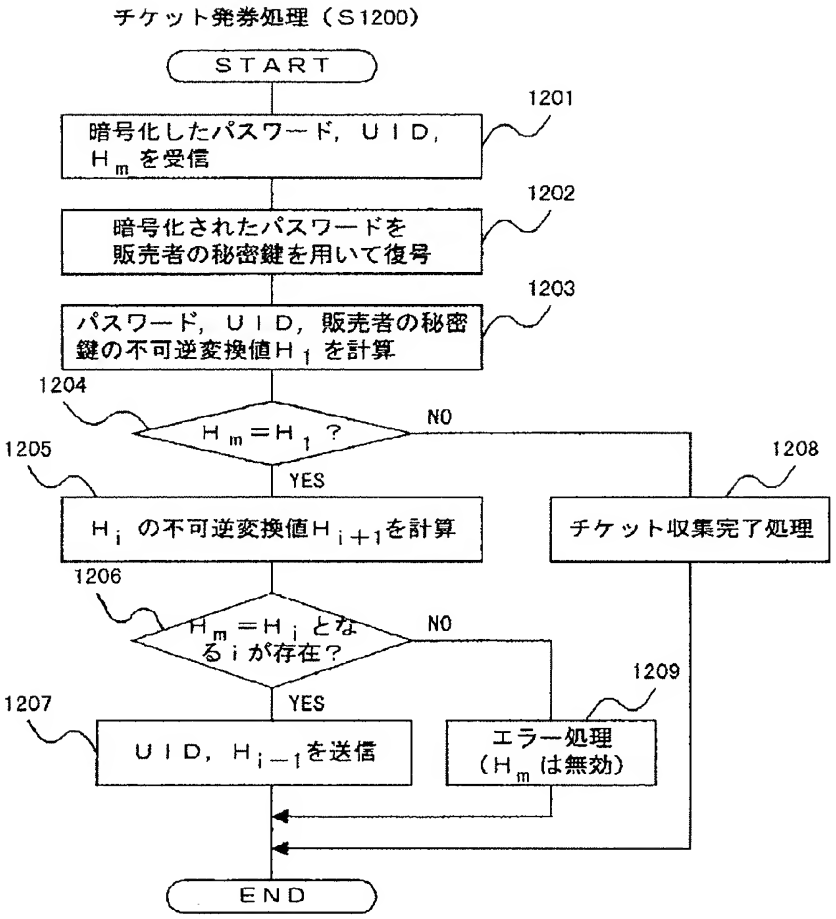

【図２６】

図 26



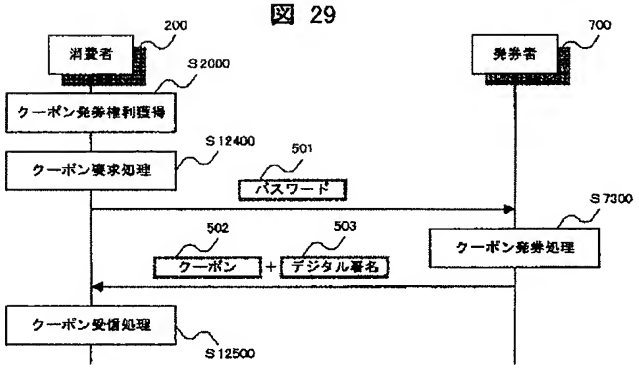
【図２３】

図 23



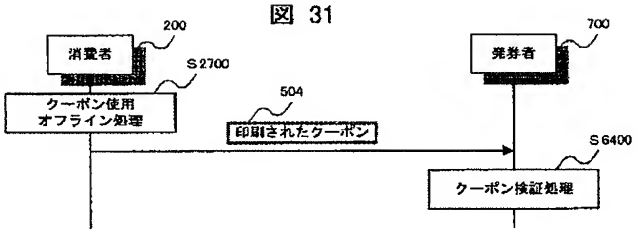

【図２９】

図 29



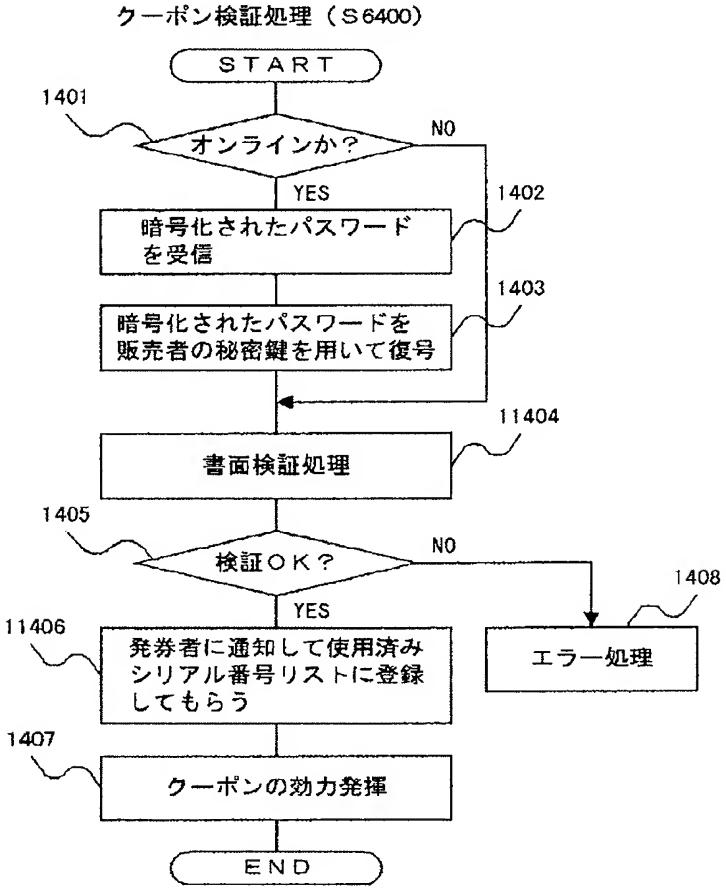
【図３１】

図 31



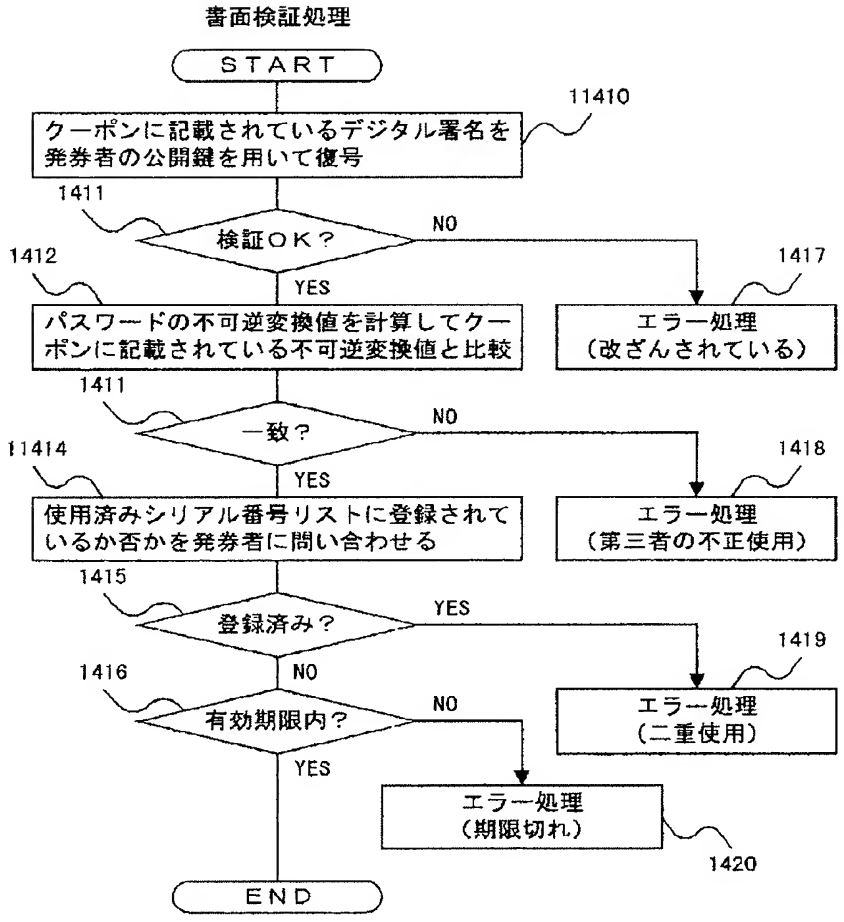

【図３２】

図 32



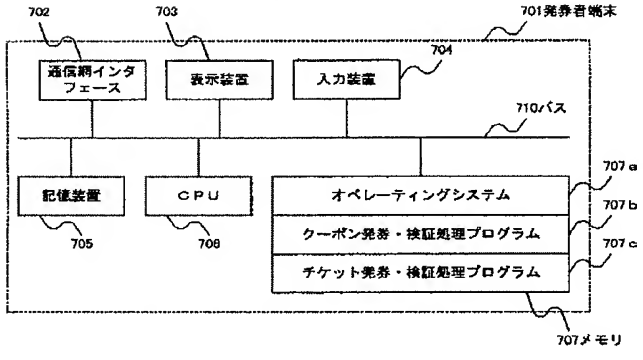
【図３３】

図 33



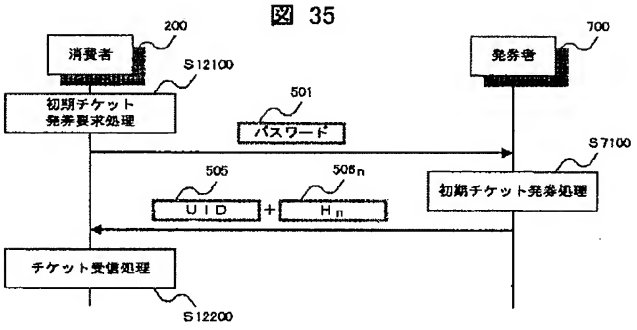

【図３４】

図 34



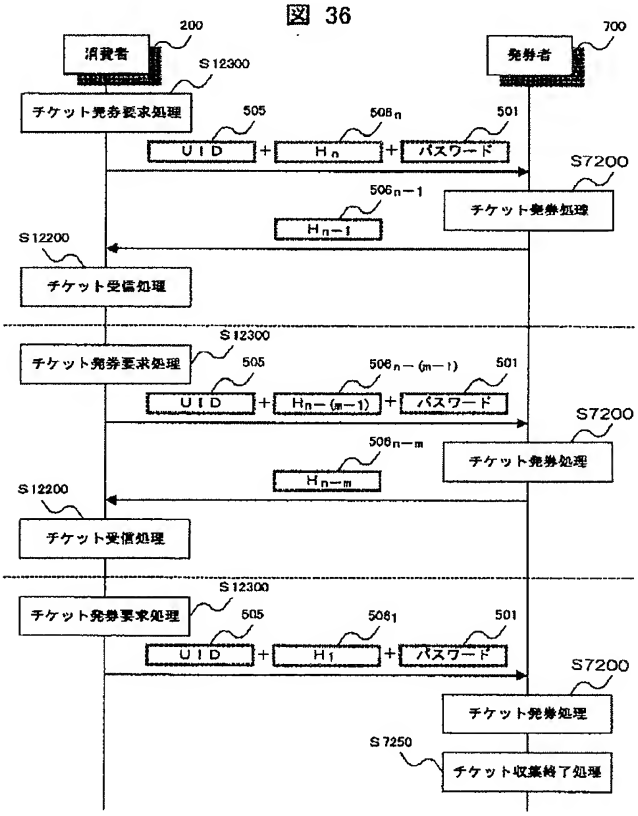
【図３５】

図 35




【図３６】

図 36




フロントページの続き

(72)発明者　豊島　久
東京都江島区新砂一丁目６番27号　株式会
社日立製作所公共情報事業部内

(72)発明者　齋藤　司
東京都江島区新砂一丁目６番27号　株式会
社日立製作所公共情報事業部内

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-328269
(43)Date of publication of application : 30.11.1999

(51)Int.Cl. G06F 17/60
G07F 7/08
G07G 1/12
G09C 1/00
H04L 9/32

(21)Application number : 10-133550
(22)Date of filing : 15.05.1998

(71)Applicant : HITACHI LTD
(72)Inventor : UMEZAWA KATSUYUKI
SUZAKI SEIICHI
YOSHIURA YUTAKA
TOYOSHIMA HISASHI
SAITO TSUKASA

## (54) ELECTRONIC COUPON SYSTEM AND METHOD FOR ISSUING AND VERIFYING ELECTRONIC COUPON

(57)Abstract:
PROBLEM TO BE SOLVED: To detect forgery and alteration of a coupon and the illegal use of a coupon by a third person even when the coupon electronically issued is printed and used.
SOLUTION: It is possible to detect alteration and forgery of a coupon by verifying a digital signature described on the coupon even when a consumer 200 prints a coupon and uses it because a seller 100 produces a coupon on which the irreversible conversion value of a password transmitted from the consumer 200coupon information that makes trouble if it is altered and a digital signature of the coupon information are described as visually recognizable data even when it is printed at the time of issuing the coupon. Alsoit is possible to detect illegal use of a coupon by a third person by such manners that the consumer 200 presents the same password as at the time of being issued when the consumer uses it and that the seller 100 compares the irreversible conversion value of the presented password with an irreversible conversion value described on the coupon.

## CLAIMS

[Claim(s)]
[Claim 1]A coupon issuing means which is equipped with the following and to which

the above-mentioned seller terminal transmits a coupon in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminala coupon in which it was transmitted from the above-mentioned consumer terminaland use was demanded -- andHave a coupon verifying means which verifies a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedand a coupon issuing means of the above-mentioned seller terminalAn irreversible transformation value of a password which received a password transmitted from the above-mentioned consumer terminaland was receivedCoupon information about effect of a couponand encipherment information enciphered using a secret encryption key with which only a vender knows this coupon informationCreate a coupon indicated as data which can be viewedtransmit to this consumer terminaland a created coupon a coupon verifying means of the above-mentioned seller terminalAn irreversible transformation value of a password which received a password and a coupon which have been transmitted from this consumer terminaland was received when a coupon in which it was transmitted from the above-mentioned consumer terminaland use was demanded was verifiedVerify whether an irreversible transformation value indicated on a received coupon is in agreementand coupon information indicated on a received couponEncipherment information enciphered using a secret encryption key which only a vender knowsIt is verified whether encipherment information indicated on a received coupon is in agreementAn irreversible transformation value of a password which acquired an irreversible transformation valuecoupon informationand encipherment information which are indicated on a printed coupon when verifying a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedand was presented by consumersAn electronic coupon system verifying whether it verifies whether an acquired irreversible transformation value is in agreementand encipherment information enciphered using a secret encryption key with which only a vender knows acquired coupon informationand acquired encipherment information are in agreement.

At least one consumer terminal which consumers use.

A coupon issue-of-banknotes request means which requires the issue of banknotes of a coupon which demonstrates effect which it came to connect mutually at least one seller terminal which a vender uses via a networkand the above-mentioned consumer terminal transmitted consumers' password to the above-mentioned seller terminaland was beforehand defined by one sheet.

A coupon reception means which receives a coupon transmitted from the above-mentioned seller terminal.

A coupon using request means to transmit consumers' password and a coupon which the above-mentioned coupon reception means received to the above-mentioned seller terminaland to require use of this couponand a coupon printing means which prints a coupon which the above-mentioned coupon reception means received.

[Claim 2]A coupon issuing means which is equipped with the following and to which the above-mentioned seller terminal transmits a coupon in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminala coupon in which it was transmitted from the above-mentioned consumer terminaland use was demanded -- andHave a coupon verifying means which verifies a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedand a coupon issuing means of the above-mentioned seller terminalAn irreversible transformation value of a password which received a password transmitted from the above-mentioned consumer terminaland was receivedA digital signature which connected coupon information about effect of a coupon and enciphered a connected result using a vender's secret key in a public-key crypto systemCreate a coupon which indicated the above-mentioned coupon information as data which can be viewedtransmit to this consumer terminaland a created coupon a coupon verifying means of the above-mentioned seller terminalWhen verifying a coupon in which it was transmitted from the above-mentioned consumer terminaland use was demandedAn irreversible transformation value of a password obtained as a result of decoding a digital signature which receives a password and a coupon which have been transmitted from this consumer terminaland is indicated on a received coupon using a vender's public key in a public-key crypto systemVerify whether an irreversible transformation value of a received password is in agreementand. Coupon information acquired as a result of decoding a digital signature indicated on a received coupon using a vender's public key in a public-key crypto systemIt is verified whether coupon information indicated on a received coupon is in agreementWhen verifying a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedAn irreversible transformation value of a password which acquires coupon information and a digital signature which are indicated on a printed couponand is obtained as a result of decoding an acquired digital signature using a vender's public key in a public-key crypto systemVerify whether an irreversible transformation value of a password presented by consumers is in agreementand. An electronic coupon system verifying whether coupon information acquired as a result of decoding an acquired digital signature using a vender's public key in a public-key crypto systemand acquired coupon information are in agreement.
At least one consumer terminal which consumers use.
A coupon issue-of-banknotes request means which requires the issue of banknotes of a coupon which demonstrates effect which it came to connect mutually at least one seller terminal which a vender uses via a networkand the above-mentioned consumer terminal transmitted consumers' password to the above-mentioned seller terminaland was beforehand defined by one sheet.
A coupon reception means which receives a coupon transmitted from the above-mentioned seller terminal.
A coupon using request means to transmit consumers' password and a coupon which the above-mentioned coupon reception means received to the above-

mentioned seller terminaland to require use of this couponand a coupon printing means which prints a coupon which the above-mentioned coupon reception means received.

[Claim 3]Are the electronic coupon system according to claim 1 or 2and a coupon issuing means of the above-mentioned seller terminalA coupon which transmitted a digital signature which enciphered this whole coupon with a created coupon using a vender's secret key in a public-key crypto system to the above-mentioned consumer terminaland received a coupon reception means of the above-mentioned consumer terminalAn electronic coupon system verifying whether a result of having decoded a transmitted digital signature using a vender's public key in a public-key crypto system with this coupon is in agreement.
[Claim 4]Are the electronic coupon system according to claim 12or 3and the above-mentioned coupon informationFor every couponincluding a peculiar serial number the above-mentioned seller terminalHave a serial number storage means which memorizes a serial number in coupon information indicated on a coupon whose effect has been demonstratedand a coupon verifying means of the above-mentioned seller terminalAn electronic coupon system verifying whether the above-mentioned serial number storage means is ending with memory about a serial number in coupon information indicated on a coupon of a verification object.
[Claim 5]An initial ticket issuing means which is equipped with the following and to which the above-mentioned seller terminal transmits the 1st ticket in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminalHave a ticket issuing means which transmits a ticket after the 2nd sheet as which the issue of banknotes was required from the above-mentioned consumer terminal to this consumer terminaland an initial ticket issuing means of the above-mentioned seller terminalA password which received a password transmitted from the above-mentioned consumer terminaland was receivedA peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsConnect secret information which only a vender knows and based on irreversible transformation value $H_1$ of a connected resultCalculate irreversible transformation value $H_{i+1}$ of irreversible transformation value $H_i$ ($1 <= i < n$) one by oneand the above UID and irreversible transformation value $H_n$ as the 1st ticketTransmit to this consumer terminal and a ticket issuing means of the above-mentioned seller terminalReceive a password and the issued banknotes newest ticket which have been transmitted from the above-mentioned consumer terminalconnect a received passwordUID of the received issued banknotes newest ticketsand secret information which only a vender knowsand based on irreversible transformation value $H_1$ of a connected resultIf irreversible transformation value $H_{i+1}$ of irreversible transformation value $H_i$ ($1 <= i < n$) is calculated one by one and irreversible transformation value $H_m$ ($1 <= m <= n$) of the received issued banknotes newest tickets and irreversible transformation value $H_1$ are in agreementAn electronic coupon system which completes the issue of banknotes of n ticketsand will be characterized by transmitting the above UID and irreversible transformation

value $H_{m-1}$ to this consumer terminal as a following ticket if not in agreement.
Are the electronic coupon system according to claim 123or 4and the above-mentioned consumer terminalAn initial ticket issue-of-banknotes request means which requires the issue of banknotes of a ticket of the 1st sheet of the coupons (a "ticket" is called hereafter.) which demonstrate effect beforehand defined when only n (n> 1) ** which transmitted consumers' password and were defined beforehand were collected to the above-mentioned seller terminal.
It is consumers' password to the above-mentioned seller terminal.
A ticket issue-of-banknotes request means which transmits a ticket (the "issued banknotes newest ticket" is called hereafter.) of the newest of the tickets issued banknotesand requires the issue of banknotes of a ticket after the 2nd sheet.
A ticket reception means which receives and saves a ticket transmitted from the above-mentioned seller terminal.

[Claim 6]An initial ticket issuing means which is equipped with the following and to which the above-mentioned seller terminal transmits the 1st ticket in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminalHave a ticket issuing means which transmits a ticket after the 2nd sheet as which the issue of banknotes was required from the above-mentioned consumer terminal to this consumer terminaland an initial ticket issuing means of the above-mentioned seller terminalA password which received a password transmitted from the above-mentioned consumer terminaland was receivedCalculate encipherment information $H_1$ which enciphered a result which connected a peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsand was connected using a secret encryption key which only a vender knowsand. Based on calculated encipherment information $H_1$calculate encipherment information $H_{i+1}$ of encipherment information $H_i$ ($1 <= i < n$) one by oneand the above UID and encipherment information $H_n$ as the 1st ticketTransmit to this consumer terminaland a ticket issuing means of the above-mentioned seller terminal receives a password and the issued banknotes newest ticket which have been transmitted from the above-mentioned consumer terminaland connects a received password and UID of the received issued banknotes newest ticketsCalculate encipherment information $H_1$ which enciphered a connected result using a secret encryption key which only a vender knowsand. Encipherment information $H_m$ ($1 <= m <= n$) of the issued banknotes newest tickets which calculated encipherment information $H_{i+1}$ of encipherment information $H_i$ ($1 <= i < n$) one by oneand were received based on calculated encipherment information $H_1$An electronic coupon system which completes the issue of banknotes of n ticketsand will be characterized by transmitting the above UID and encipherment information $H_{m-1}$ to this consumer terminal as a following ticket if not in agreement if encipherment information $H_1$ is in agreement.
Are the electronic coupon system according to claim 123or 4and the above-mentioned consumer terminalAn initial ticket issue-of-banknotes request means which requires the issue of banknotes of a ticket of the 1st sheet of the coupons

(a "ticket" is called hereafter.) which demonstrate effect beforehand defined when only n (n> 1) ** which transmitted consumers' password and were defined beforehand were collected to the above-mentioned seller terminal.
It is consumers' password to the above-mentioned seller terminal.
A ticket issue-of-banknotes request means which transmits a ticket (the "issued banknotes newest ticket" is called hereafter.) of the newest of the tickets issued banknotesand requires the issue of banknotes of a ticket after the 2nd sheet.
A ticket reception means which receives and saves a ticket transmitted from the above-mentioned seller terminal.

[Claim 7]An initial ticket issuing means which is equipped with the following and to which the above-mentioned seller terminal transmits the 1st ticket in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminalHave a ticket issuing means which transmits a ticket after the 2nd sheet as which the issue of banknotes was required from the above-mentioned consumer terminal to this consumer terminaland an initial ticket issuing means of the above-mentioned seller terminalA password which received a password transmitted from the above-mentioned consumer terminaland was receivedA peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsEncipherment information $H_1$ which enciphered a result which connected number-of-sheets information which shows that it is the 1st ticketand was connected using a secret encryption key which only a vender knows as the 1st ticketTransmit to this consumer terminal and a ticket issuing means of the above-mentioned seller terminalA password and the issued banknotes newest ticket which have been transmitted from the above-mentioned consumer terminal are receivedIf number-of-sheets information acquired as a result of decoding encipherment information $H_m$ (1 <=m<=n) which receivedand which is the issued banknotes newest ticket using a secret encryption key which only a vender knows is number-of-sheets information which shows that it is the n-th ticketthe issue of banknotes of n tickets will be completedUID obtained as a result of decoding a received password and encipherment information $H_m$ (1 <=m<=n) which receivedand which is the issued banknotes newest tickets using a secret encryption key which only a vender knowsif that was not rightAn electronic coupon system transmitting encipherment information $H_{m+1}$ which enciphered a result which connected number-of-sheets information which shows that they are the m+1st ticketsand was connected using a secret encryption key which only a vender knows to this consumer terminal as a following ticket.
Are the electronic coupon system according to claim 123or 4and the above-mentioned consumer terminalAn initial ticket issue-of-banknotes request means which requires the issue of banknotes of a ticket of the 1st sheet of the coupons (a "ticket" is called hereafter.) which demonstrate effect beforehand defined when only n (n> 1) ** which transmitted consumers' password and were defined beforehand were collected to the above-mentioned seller terminal.
It is consumers' password to the above-mentioned seller terminal.

A ticket issue-of-banknotes request means which transmits a ticket (the "issued banknotes newest ticket" is called hereafter.) of the newest of the tickets issued banknotesand requires the issue of banknotes of a ticket after the 2nd sheet.
A ticket reception means which receives and saves a ticket transmitted from the above-mentioned seller terminal.

[Claim 8]Are the electronic coupon system according to claim 123456or 7and the above-mentioned consumer terminalWhen transmitting a password to the above-mentioned seller terminalTransmitafter enciphering this password using a vender's public key in a public-key crypto systemand the above-mentioned seller terminalAn electronic coupon system characterized by decoding this password using a vender's secret key in a public-key crypto system when a password transmitted from the above-mentioned consumer terminal is received.
[Claim 9]Have the followingand the above-mentioned issue-of-banknotes person terminal is provided with a coupon issuing means which transmits a coupon in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminaland the above-mentioned seller terminala coupon in which it was transmitted from the above-mentioned consumer terminaland use was demanded -- andHave a coupon verifying means which verifies a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedand a coupon issuing means of the above-mentioned issue-of-banknotes person terminalAn irreversible transformation value of a password which received a password transmitted from the above-mentioned consumer terminaland was receivedA digital signature enciphered using a secret key [ in / for coupon information about effect and this coupon information of a coupon / a public-key crypto system ] of an issue-of-banknotes personCreate a coupon indicated as data which can be viewedtransmit to this consumer terminaland a created coupon a coupon verifying means of the above-mentioned seller terminalAn irreversible transformation value of a password which received a password and a coupon which have been transmitted from this consumer terminaland was received when a coupon in which it was transmitted from the above-mentioned consumer terminaland use was demanded was verifiedVerify whether an irreversible transformation value indicated on a received coupon is in agreementand a digital signature indicated on a received couponIt is verified whether a result decoded using a public key of an issue-of-banknotes person in a public-key crypto system and coupon information indicated on a received coupon are in agreementAn irreversible transformation value of a password which acquired an irreversible transformation valuecoupon informationand a digital signature which are indicated on a printed coupon when verifying a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedand was presented by consumersAn electronic coupon system verifying whether it verifies whether an acquired irreversible transformation value is in agreementand a result of having decoded an acquired digital signature using a public key of an issue-of-banknotes person in a public-key crypto systemand acquired coupon information

are in agreement.
At least one consumer terminal which consumers use.
At least one seller terminal which a vender uses.
A coupon issue-of-banknotes request means which requires the issue of banknotes of a coupon which demonstrates effect which it came to connect mutually at least one issue-of-banknotes person terminal which an issue-of-banknotes person uses via a networkand the above-mentioned consumer terminal transmitted consumers' password to the above-mentioned issue-of-banknotes person terminaland was beforehand defined by one sheet.
A coupon reception means which receives a coupon transmitted from the above-mentioned issue-of-banknotes person terminalA coupon using request means to transmit consumers' password and a coupon which the above-mentioned coupon reception means received to the above-mentioned seller terminaland to require use of this couponand a coupon printing means which prints a coupon which the above-mentioned coupon reception means received.

[Claim 10]Have the followingand the above-mentioned issue-of-banknotes person terminal is provided with a coupon issuing means which transmits a coupon in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminaland the above-mentioned seller terminala coupon in which it was transmitted from the above-mentioned consumer terminaland use was demanded -- andHave a coupon verifying means which verifies a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedand a coupon issuing means of the above-mentioned issue-of-banknotes person terminalAn irreversible transformation value of a password which received a password transmitted from the above-mentioned consumer terminaland was receivedA digital signature which connected coupon information about effect of a coupon and enciphered a connected result using a secret key of an issue-of-banknotes person in a public-key crypto systemCreate a coupon which indicated this coupon information as data which can be viewedtransmit to this consumer terminaland a created coupon a coupon verifying means of the above-mentioned seller terminalWhen verifying a coupon in which it was transmitted from the above-mentioned consumer terminaland use was demandedAn irreversible transformation value of a password obtained as a result of decoding a digital signature which receives a password and a coupon which have been transmitted from this consumer terminaland is indicated on a received coupon using a public key of an issue-of-banknotes person in a public-key crypto systemVerify whether an irreversible transformation value of a received password is in agreementand. Coupon information acquired as a result of decoding a digital signature indicated on a received coupon using a public key of an issue-of-banknotes person in a public-key crypto systemIt is verified whether coupon information indicated on a received coupon is in agreementWhen verifying a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedAn irreversible transformation value of a password which

acquires coupon information and a digital signature which are indicated on a printed couponand is obtained as a result of decoding an acquired digital signature using a public key of an issue-of-banknotes person in a public-key crypto systemVerify whether an irreversible transformation value of a password presented by consumers is in agreementand. An electronic coupon system verifying whether coupon information acquired as a result of decoding an acquired digital signature using a public key of an issue-of-banknotes person in a public-key crypto systemand acquired coupon information are in agreement.
At least one consumer terminal which consumers use.
At least one seller terminal which a vender uses.
A coupon issue-of-banknotes request means which requires the issue of banknotes of a coupon which demonstrates effect which it came to connect mutually at least one issue-of-banknotes person terminal which an issue-of-banknotes person uses via a networkand the above-mentioned consumer terminal transmitted consumers' password to the above-mentioned issue-of-banknotes person terminaland was beforehand defined by one sheet.
A coupon reception means which receives a coupon transmitted from the above-mentioned issue-of-banknotes person terminalA coupon using request means to transmit consumers' password and a coupon which the above-mentioned coupon reception means received to the above-mentioned seller terminaland to require use of this couponand a coupon printing means which prints a coupon which the above-mentioned coupon reception means received.

[Claim 11]Are the electronic coupon system according to claim 9 or 10and a coupon issuing means of the above-mentioned issue-of-banknotes person terminalA coupon which transmitted a digital signature which enciphered this whole coupon with a created coupon using a secret key of an issue-of-banknotes person in a public-key crypto system to the above-mentioned consumer terminaland received a coupon reception means of the above-mentioned consumer terminalAn electronic coupon system verifying whether a result of having decoded a transmitted digital signature using a public key of an issue-of-banknotes person in a public-key crypto system with this coupon is in agreement.
[Claim 12]Have the following and a coupon verifying means of the above-mentioned seller terminalNotify a serial number in coupon information indicated on a coupon whose effect has been demonstrated to the above-mentioned issue-of-banknotes person terminaland. An electronic coupon system asking a verification result about a serial number in coupon information indicated on a coupon of a verification object to the above-mentioned issue-of-banknotes person terminal.
A serial number storage means with which are the electronic coupon system according to claim 910or 11and the above-mentioned coupon information remembers a serial number it was notified from the above-mentioned seller terminal including a peculiar serial number for every coupon that the above-mentioned issue-of-banknotes person terminal was to be.
A serial number verifying means which verifies whether the above-mentioned

serial number storage means is ending with memory about a serial number which had an inquiry from the above-mentioned seller terminaland answers a verification result to this seller terminal.

[Claim 13]An initial ticket issuing means which is equipped with the following and to which the above-mentioned issue-of-banknotes person terminal transmits the 1st ticket in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminalHave a ticket issuing means which transmits a ticket after the 2nd sheet as which the issue of banknotes was required from the above-mentioned consumer terminal to this consumer terminaland an initial ticket issuing means of the above-mentioned issue-of-banknotes person terminalA password which received a password transmitted from the above-mentioned consumer terminaland was receivedA peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsConnect secret information which only an issue-of-banknotes person knowsand based on irreversible transformation value $H_1$ of a connected resultCalculate irreversible transformation value $H_{i+1}$ of irreversible transformation value $H_i$ ($1 <= i < n$) one by oneand the above UID and irreversible transformation value $H_n$ as the 1st ticketTransmit to this consumer terminal and a ticket issuing means of the above-mentioned issue-of-banknotes person terminalReceive a password and the issued banknotes newest ticket which have been transmitted from the above-mentioned consumer terminalconnect a received passwordUID of the received issued banknotes newest ticketsand secret information which only an issue-of-banknotes person knowsand based on irreversible transformation value $H_1$ of a connected resultIf irreversible transformation value $H_{i+1}$ of irreversible transformation value $H_i$ ($1 <= i < n$) is calculated one by one and irreversible transformation value $H_m$ ($1 <= m <= n$) of the received issued banknotes newest tickets and irreversible transformation value $H_1$ are in agreementAn electronic coupon system which completes the issue of banknotes of n ticketsand will be characterized by transmitting the above UID and irreversible transformation value $H_{m-1}$ to this consumer terminal as a following ticket if not in agreement.
Are the electronic coupon system according to claim 91011or 12and the above-mentioned consumer terminalAn initial ticket issue-of-banknotes request means which requires the issue of banknotes of a ticket of the 1st sheet of the coupons (a "ticket" is called hereafter.) which demonstrate effect beforehand defined when only n ($n > 1$) ** which transmitted consumers' password and were defined beforehand were collected to the above-mentioned issue-of-banknotes person terminal.
It is consumers' password to the above-mentioned issue-of-banknotes person terminal.
A ticket issue-of-banknotes request means which transmits a ticket (the "issued banknotes newest ticket" is called hereafter.) of the newest of the tickets issued banknotesand requires the issue of banknotes of a ticket after the 2nd sheet.
A ticket reception means which receives and saves a ticket transmitted from the

above-mentioned issue-of-banknotes person terminal.

[Claim 14]An initial ticket issuing means which is equipped with the following and to which the above-mentioned issue-of-banknotes person terminal transmits the 1st ticket in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminalHave a ticket issuing means which transmits a ticket after the 2nd sheet as which the issue of banknotes was required from the above-mentioned consumer terminal to this consumer terminaland an initial ticket issuing means of the above-mentioned issue-of-banknotes person terminalA password which received a password transmitted from the above-mentioned consumer terminaland was receivedCalculate encipherment information $H_1$ which enciphered a result which connected a peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsand was connected using a secret encryption key which only an issue-of-banknotes person knowsand. Based on calculated encipherment information $H_1$calculate encipherment information $H_{i+1}$ of encipherment information $H_i$ ($1 <= i < n$) one by oneand the above UID and encipherment information $H_n$ as the 1st ticketTransmit to this consumer terminaland a ticket issuing means of the above-mentioned issue-of-banknotes person terminal receives a password and the issued banknotes newest ticket which have been transmitted from the above-mentioned consumer terminaland connects a received password and UID of the received issued banknotes newest ticketsCalculate encipherment information $H_1$ which enciphered a connected result using a secret encryption key which only an issue-of-banknotes person knowsand. Encipherment information $H_m$ ($1 <= m <= n$) of the issued banknotes newest tickets which calculated encipherment information $H_{i+1}$ of encipherment information $H_i$ ($1 <= i < n$) one by oneand were received based on calculated encipherment information $H_1$An electronic coupon system which completes the issue of banknotes of n ticketsand will be characterized by transmitting the above UID and encipherment information $H_{m-1}$ to this consumer terminal as a following ticket if not in agreement if encipherment information $H_1$ is in agreement.
Are the electronic coupon system according to claim 91011or 12and the above-mentioned consumer terminalAn initial ticket issue-of-banknotes request means which requires the issue of banknotes of a ticket of the 1st sheet of the coupons (a "ticket" is called hereafter.) which demonstrate effect beforehand defined when only n ($n > 1$) ** which transmitted consumers' password and were defined beforehand were collected to the above-mentioned issue-of-banknotes person terminal.
It is consumers' password to the above-mentioned issue-of-banknotes person terminal.
A ticket issue-of-banknotes request means which transmits a ticket (the "issued banknotes newest ticket" is called hereafter.) of the newest of the tickets issued banknotesand requires the issue of banknotes of a ticket after the 2nd sheet.
A ticket reception means which receives and saves a ticket transmitted from the

above-mentioned issue-of-banknotes person terminal.

[Claim 15]An initial ticket issuing means which is equipped with the following and to which the above-mentioned issue-of-banknotes person terminal transmits the 1st ticket in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminalHave a ticket issuing means which transmits a ticket after the 2nd sheet as which the issue of banknotes was required from the above-mentioned consumer terminal to this consumer terminaland an initial ticket issuing means of the above-mentioned issue-of-banknotes person terminalA password which received a password transmitted from the above-mentioned consumer terminaland was receivedA peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsEncipherment information $H_1$ which enciphered a result which connected number-of-sheets information which shows that it is the 1st ticketand was connected using a secret encryption key which only an issue-of-banknotes person knows as the 1st ticketTransmit to this consumer terminal and a ticket issuing means of the above-mentioned issue-of-banknotes person terminalA password and the issued banknotes newest ticket which have been transmitted from the above-mentioned consumer terminal are receivedIf number-of-sheets information acquired as a result of decoding encipherment information $H_m$ (1 <=m<=n) which receivedand which is the issued banknotes newest ticket using a secret encryption key which only an issue-of-banknotes person knows is number-of-sheets information which shows that it is the n-th ticketthe issue of banknotes of n tickets will be completedUID obtained as a result of decoding a received password and encipherment information $H_m$ (1 <=m<=n) which receivedand which is the issued banknotes newest tickets using a secret encryption key which only an issue-of-banknotes person knowsif that was not rightAn electronic coupon system transmitting encipherment information $H_{m+1}$ which enciphered a result which connected number-of-sheets information which shows that they are the m+1st ticketsand was connected using a secret encryption key which only an issue-of-banknotes person knows to this consumer terminal as a following ticket.
Are the electronic coupon system according to claim 91011or 12and the above-mentioned consumer terminalAn initial ticket issue-of-banknotes request means which requires the issue of banknotes of a ticket of the 1st sheet of the coupons (a "ticket" is called hereafter.) which demonstrate effect beforehand defined when only n (n> 1) ** which transmitted consumers' password and were defined beforehand were collected to the above-mentioned issue-of-banknotes person terminal.
It is consumers' password to the above-mentioned issue-of-banknotes person terminal.
A ticket issue-of-banknotes request means which transmits a ticket (the "issued banknotes newest ticket" is called hereafter.) of the newest of the tickets issued banknotesand requires the issue of banknotes of a ticket after the 2nd sheet.
A ticket reception means which receives and saves a ticket transmitted from the

above-mentioned seller terminal.

[Claim 16]Are the electronic coupon system according to claim 91011121314or 15and the above-mentioned consumer terminalWhen transmitting a password to the above-mentioned issue-of-banknotes person terminalWhen transmitting after enciphering this password using a public key of an issue-of-banknotes person in a public-key crypto systemand transmitting a password to the above-mentioned seller terminalTransmitafter enciphering this password using a vender's public key in a public-key crypto systemand the above-mentioned issue-of-banknotes person terminalWhen a password transmitted from the above-mentioned consumer terminal is receivedAn electronic coupon system when this password is decoded using a secret key of an issue-of-banknotes person in a public-key crypto systemand the above-mentioned seller terminal receives a password transmitted from the above-mentioned consumer terminalwherein it decodes this password using a vender's secret key in a public-key crypto system.
[Claim 17]In a system which comes to connect mutually at least one consumer terminal which consumers useand at least one seller terminal which a vender uses via a networkBy one sheetare the method of performing the issue of banknotes and verification of a coupon which demonstrate effect defined beforehandand at the time of the issue of banknotes of a coupon the above-mentioned seller terminalA password which received a password transmitted from a consumer terminal which required the issue of banknotes of a couponand was receivedEncipherment information which is the result of enciphering coupon information about effect of a coupon with an encryption method which only self can encipherand encipheringCreate a coupon which indicated this coupon information as data which can be viewedtransmit to a consumer terminal and a created coupon at the time of verification of a coupon the above-mentioned seller terminalIn being the coupon in which a coupon of a verification object was transmitted from the above-mentioned consumer terminaland use was demandedA result which received a password and a coupon which are transmitted from this consumer terminalenciphered a password and coupon information which were received with the same encryption method as the time of the issue of banknotes of a couponand was encipheredEncipherment information indicated on a received coupon verifies whether it is in agreementand a coupon of a verification objectIn being the coupon in which it was printed with the above-mentioned consumer terminaland use was demandedA result which acquired coupon information and encipherment information which are indicated on a printed couponenciphered a password presented by consumers and acquired coupon information with the same encryption method as the time of the issue of banknotes of a couponand was encipheredThe electronic coupon issue of banknotes and a detecting method verifying whether acquired encipherment information is in agreement.
[Claim 18]In a system which comes to connect mutually at least one consumer terminal which consumers useat least one seller terminal which a vender usesand at least one issue-of-banknotes person terminal which an issue-of-banknotes

person uses via a networkBy one sheetare the method of performing the issue of banknotes and verification of a coupon which demonstrate effect defined beforehandand at the time of the issue of banknotes of a coupon the above-mentioned issue-of-banknotes person terminalA password which received a password transmitted from a consumer terminal which required the issue of banknotes of a couponand was receivedEncipherment information which is the result of enciphering coupon information about effect of a coupon with an encryption method which only self can encipherand encipheringCreate a coupon which indicated this coupon information as data which can be viewedtransmit to a consumer terminal and a created coupon at the time of verification of a coupon the above-mentioned seller terminalIn being the coupon in which a coupon of a verification object was transmitted from the above-mentioned consumer terminaland use was demandedReceive a password and a coupon which are transmitted from this consumer terminaltransmit a password and coupon information which were received to the above-mentioned issue-of-banknotes person terminalrequire verification of this couponand a coupon of a verification objectIn being the coupon in which it was printed with the above-mentioned consumer terminaland use was demandedAcquire a printed coupontransmit a password presented by consumers and an acquired coupon to the above-mentioned issue-of-banknotes person terminalrequire verification of this couponand the above-mentioned issue-of-banknotes person terminalA result of having received a password and a coupon which are transmitted from a seller terminal which required verification of a couponand having enciphered a password and coupon information which were received with the same encryption method as the time of the issue of banknotes of a couponThe electronic coupon issue of banknotes and a detecting method verifying whether encipherment information indicated on a received coupon is in agreementand notifying a verification result to this seller terminal.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]In the utilizing environment of the electronic commerce system with which this invention is performed via networkssuch as the InternetVarious goodsand service and an exchangeable electronic coupon about the electronic coupon system for dealing with it properly in more detailThe consumers who received the electronic coupon via the network are related with the electronic coupon system which enabled it to use this electronic coupon not only in the virtual store established on the network but in the store which exists actually.

[0002]

[Description of the Prior Art]Nowthe ticket (a "coupon" is called generally

hereafter.) exchangeable for various goods and servicessuch as a gift certificate and a discount tickethas spread. Although there are what demonstrates effect by one sheetand a thing which demonstrates effect when only two or more sheets are collected in this kind of couponHe is trying to prevent a third party's unauthorized use by being made to make forgery and an alteration difficult by using advanced printing techniqueor checking a signature at the time of useso that effect becomes large.

[0003]By the wayelectronic commerce technology through an open network like the Internet is briskly performed increasingly by development of information machines and equipment in recent yearsand maintenance of communication environment. On a networka vender establishes a virtual store and sells goods to general consumers.

[0004]Also in the electronic commerce technology through such a networkthe demand of liking to deal with a coupon (electronic coupon) as part of consumer services is increasing. Howeverwhen an electronic coupon is made into mere image datait will be able to perform simply that copy the electronic couponand the consumers who received the electronic coupon in the regular procedure use it repeatedlyand supply other consumers widely. Since an electronic coupon is distributed via an open networkthere is also a possibility that it may be intercepted and used improperly by the third party.

[0005]As a measure for preventing such a malfeasancethe following encoding technology is used in the electronic coupon system.

[0006]In order to prevent forgery and an alteration of an electronic coupon in an electronic coupon system as the 1st measurehe adds a vender's (agency issuing banknotes) digital signature to an electronic couponand is trying to check the digital signature at the time of use. Digital signature art is indicated by 133 pages - 138 pages of "code theoretical introduction:Eiji Okamoto work and KYORITSU SHUPPAN (1996)"for example. It is as follows if the signature method by the asymmetric cipher (public key encryption) in this literature is explained briefly.

[0007]A signer is enciphering a message (or hash value of a message) to sign using the secret key which only a signer knowshe creates signature dataputs a message and signature data togetherand hands a verification person. If a verification person's message which decoded the received signature data using the public key corresponding to the above-mentioned secret keyand thought it to be the decoded result correspondshe will judge that it is the data signed by the above-mentioned signer.

[0008]In order to prevent double use of an electronic coupon in an electronic coupon system as the 2nd measurehe adds a serial number to each electronic couponand is trying to check whether it is an intact electronic coupon with checking the serial number at the time of use.

[0009]In order to prevent the unauthorized use of the electronic coupon by a third party in an electronic coupon system as the 3rd measurehe enciphers a message and is trying to transmit. As a method of enciphering a messageSSL (Secure Socket Layer) etc. which are indicated to 101 pages - 112 pages of a

"OpenDesign(No. 1996/6 No.14):CQ publishing company" are mentionedfor example.
[0010]
[Problem(s) to be Solved by the Invention]In the case of a system only for an electronic coupon which performs all the processings from the issue of banknotes of an electronic coupon to use via a networkvarious malfeasances can be prevented by taking all the measures mentioned above. Howeverif consumers' user-friendliness is taken into considerationthe electronic coupon which consumers received via the network will be printed on paperAlthough the paper coupon and an electronic coupon concomitant use system which is brought and used for a store are preferred like the coupon of the conventional paper basisin being such a systemSince the digital signature added to the electronic coupon is not reflected in a printed resultforgery of an electronic coupon cannot be prevented.
[0011]Although double use of a coupon can be prevented by managing a used serial number in a storeIf a third party uses the coupon improperly when the memory storage of a consumer terminal is robbed of the electronic coupon received via the networkor when the printed coupon is stolenit will become impossible for just consumers to use a coupon.
[0012]When only two or more sheets are collectedin dealing with a coupon (this kind of coupon is hereafter called a "ticket".) which demonstrates effectSince issue-of-banknotes number of sheets increases compared with the coupon which demonstrates effect by one sheet and all consumers do not finish collecting ticketsit is serious to manage by the vender side for every consumers.
[0013]in light of the above-mentioned circumstancesthis invention comes out. It is in the consumers who received the electronic coupon via the purpose providing the electronic coupon system which enabled it to use this electronic coupon not only in the virtual store established on the network but in the store which exists actually.

[0014]There are other purposes of this invention in providing the electronic coupon system which enabled it to reduce a vender's time and effortwhen dealing with a ticket.
[0015]
[Means for Solving the Problem]To achieve the above objectsat least one consumer terminal in which consumers use this invention as the 1st modeCome to be connected mutually via a network and at least one seller terminal which a vender uses the above-mentioned consumer terminalA coupon issue-of-banknotes request means which requires the issue of banknotes of a coupon which demonstrates effect which transmitted consumers' password and was beforehand defined by one sheet to the above-mentioned seller terminalA coupon reception means which receives a coupon transmitted from the above-mentioned seller terminalConsumers' password and a coupon which the above-mentioned coupon reception means received are transmitted to the above-mentioned seller

terminalHave a coupon using request means to require use of this couponand a coupon printing means which prints a coupon which the above-mentioned coupon reception means receivedand the above-mentioned seller terminalA coupon issuing means which transmits a coupon in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminalHave a coupon verifying means which verifies a coupon in which it was transmitted from the above-mentioned consumer terminaland use was demandedand a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedand a coupon issuing means of the above-mentioned seller terminal receives a password transmitted from the above-mentioned consumer terminalAn irreversible transformation value of a received passwordand coupon information about effect of a couponEncipherment information enciphered using a secret encryption key with which only a vender knows this coupon informationCreate a coupon indicated as data which can be viewedtransmit to this consumer terminaland a created coupon a coupon verifying means of the above-mentioned seller terminalAn irreversible transformation value of a password which received a password and a coupon which have been transmitted from this consumer terminaland was received when a coupon in which it was transmitted from the above-mentioned consumer terminaland use was demanded was verifiedVerify whether an irreversible transformation value indicated on a received coupon is in agreementand. Encipherment information enciphered using a secret encryption key with which only a vender knows coupon information indicated on a received couponIt is verified whether encipherment information indicated on a received coupon is in agreementAn irreversible transformation value of a password which acquired an irreversible transformation valuecoupon informationand encipherment information which are indicated on a printed coupon when verifying a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedand was presented by consumersVerify whether an acquired irreversible transformation value is in agreementand. An electronic coupon system verifying whether encipherment information enciphered using a secret encryption key with which only a vender knows acquired coupon informationand acquired encipherment information are in agreement is provided.

[0016]Since he is trying to create a coupon which indicated encipherment information which enciphered it about troubled coupon information as data which can be viewed according to the 1st mode if alteredEven when consumers print and use a couponforgery and an alteration of a coupon can be prevented by verifying encipherment information indicated on a printed coupon.

[0017]Since he is trying to create a coupon which indicated the irreversible transformation value as data which can be viewed about a password which consumers presented at the time of the issue of banknotes of a coupon according to the 1st modeAn unauthorized use of a coupon by a third party can be detected now by comparing an irreversible transformation value of a password which consumers presented at the time of use of a coupon with an irreversible

transformation value indicated on a coupon.
[0018]In the 1st modea coupon issuing means of the above-mentioned seller terminalAn irreversible transformation value of a password which received not operation mentioned above but a password transmitted from the above-mentioned consumer terminaland was receivedA digital signature which connected coupon information about effect of a coupon and enciphered a connected result using a vender's secret key in a public-key crypto systemCreate a coupon which indicated the above-mentioned coupon information as data which can be viewedand when it may be made to transmit to this consumer terminal and a created coupon is carried out in this wayWhen verifying a coupon in which it was transmitted from the above-mentioned consumer terminaland use was demandeda coupon verifying means of the above-mentioned seller terminalA password and a coupon which have been transmitted from this consumer terminal are receivedAn irreversible transformation value of a password obtained as a result of decoding a digital signature indicated on a received coupon using a vender's public key in a public-key crypto systemCoupon information acquired as a result of verifying whether an irreversible transformation value of a received password is in agreement and decoding a digital signature indicated on a received coupon using a vender's public key in a public-key crypto systemIt is verified whether coupon information indicated on a received coupon is in agreementWhen verifying a coupon in which it was printed with the above-mentioned consumer terminaland use was demandedAn irreversible transformation value of a password which acquires coupon information and a digital signature which are indicated on a printed couponand is obtained as a result of decoding an acquired digital signature using a vender's public key in a public-key crypto systemVerify whether an irreversible transformation value of a password presented by consumers is in agreementand. It can be verified whether coupon information acquired as a result of decoding an acquired digital signature using a vender's public key in a public-key crypto systemand acquired coupon information are in agreement.
[0019]In the 1st modea coupon issuing means of the above-mentioned seller terminalA digital signature which enciphered this whole coupon with a created coupon using a vender's secret key in a public-key crypto systemIt is made to transmit to the above-mentioned consumer terminaland may be made to verify whether a received coupon and result of a coupon reception means of the above-mentioned consumer terminal of having decoded a digital signature transmitted with this coupon using a vender's public key in a public-key crypto system correspond.
[0020]If it does in this waya received coupon can be verified by the consumer side who received the issue of banknotes of a coupon not only at the time of use of a coupon but at the time of the issue of banknotes of a coupon.
[0021]In the 1st modemake it the above-mentioned coupon information contain a peculiar serial number for every couponand it the above-mentioned seller terminalHave a serial number storage means which memorizes a serial number in coupon information indicated on a coupon whose effect has been

demonstratedand a coupon verifying means of the above-mentioned seller terminalIt may be made to verify whether about a serial number in coupon information indicated on a coupon of a verification objectthe above-mentioned serial number storage means is ending with memory.

[0022]If it does in this wayin addition to forgery of a couponan alterationand an unauthorized use of a coupon by a third partydouble use of a coupon can also be prevented.

[0023]In order to attain the purpose besides the abovethis inventionAs the 2nd modein the 1st modethe above-mentioned consumer terminalA coupon which demonstrates effect beforehand defined when only n (n> 1) ** which transmitted consumers' password and were defined beforehand were collected to the above-mentioned seller terminal. (a "ticket" is called hereafter.) -- with an initial ticket issue-of-banknotes request means which requires the issue of banknotes of the 1st ticket. Consumers' password and a ticket (the "issued banknotes newest ticket" is called hereafter.) of the newest of the tickets issued banknotes are transmitted to the above-mentioned seller terminalHave a ticket issue-of-banknotes request means which requires the issue of banknotes of a ticket after the 2nd sheetand a ticket reception means which receives and saves a ticket transmitted from the above-mentioned seller terminaland the above-mentioned seller terminalAn initial ticket issuing means which transmits the 1st ticket in which the issue of banknotes was demanded from the above-mentioned consumer terminal to this consumer terminalA password which it had a ticket issuing means which transmits a ticket after the 2nd sheet as which the issue of banknotes was required from the above-mentioned consumer terminal to this consumer terminaland an initial ticket issuing means of the above-mentioned seller terminal received a password transmitted from the above-mentioned consumer terminaland was receivedA peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsConnect secret information which only a vender knows and based on irreversible transformation value $H_1$ of a connected resultCalculate irreversible transformation value $H_{i+1}$ of irreversible transformation value $H_i$ (1 <=i<n) one by oneand the above UID and irreversible transformation value $H_n$ as the 1st ticketTransmit to this consumer terminal and a ticket issuing means of the above-mentioned seller terminalA password which received a password and the issued banknotes newest ticket which have been transmitted from the above-mentioned consumer terminaland was receivedUID of the received issued banknotes newest tickets and secret information which only a vender knows are connectedBased on irreversible transformation value $H_1$ of a connected resultirreversible transformation value $H_{i+1}$ of irreversible transformation value $H_i$ (1 <=i<n) is calculated one by oneIf irreversible transformation value $H_m$ (1 <=m<=n) of the received issued banknotes newest tickets and irreversible transformation value $H_1$ are in agreementcomplete the issue of banknotes of n ticketsand if not in agreementthe above UID and irreversible transformation value $H_{m-1}$ as a following ticketAn electronic coupon system transmitting to this consumer terminal is provided.

[0024]A password which is the information which only consumers know according to the 2nd modeSecret information (for examplea vender's secret key in a public-key crypto system) which only a vender knowsRepeatfrom what connected UID for identifying a group of n ticketscalculate an irreversible transformation valueand in the n-th calculation resultthe n-1st calculation results--turn of the 2nd calculation result and the 1st calculation result. Since he is trying to issue each calculation result as a ticketit becomes unnecessary to manage how many tickets were already issued for every consumers by the store side.

[0025]In the 2nd modean initial ticket issuing means of the above-mentioned seller terminalA password which received not operation mentioned above but a password transmitted from the above-mentioned consumer terminaland was receivedCalculate encipherment information $H_1$ which enciphered a result which connected a peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsand was connected using a secret encryption key which only a vender knowsand. Based on calculated encipherment information $H_1$calculate encipherment information $H_{i+1}$ of encipherment information $H_i$ ($1 <= i < n$) one by oneand the above UID and encipherment information $H_n$ as the 1st ticketMake it transmit to this consumer terminaland a ticket issuing means of the above-mentioned seller terminalA password which received not operation mentioned above but a password transmitted from the above-mentioned consumer terminaland the issued banknotes newest ticketand was receivedCalculate encipherment information $H_1$ which enciphered a result which connected UID of the received issued banknotes newest ticketsand was connected using a secret encryption key which only a vender knowsand based on calculated encipherment information $H_1$If encipherment information $H_{i+1}$ of encipherment information $H_i$ ($1 <= i < n$) is calculated one by one and encipherment information $H_m$ ($1 <= m <= n$) of the received issued banknotes newest tickets and encipherment information $H_1$ are in agreementThe issue of banknotes of n tickets is completedand if not in agreementit may be made to transmit the above UID and encipherment information $H_{m-1}$ to this consumer terminal as a following ticket.

[0026]In the 2nd modean initial ticket issuing means of the above-mentioned seller terminalNot operation mentioned above but an initial ticket issuing means of the above-mentioned seller terminalA password which received a password transmitted from the above-mentioned consumer terminaland was receivedA peculiar value ("UID" is called hereafter.) given in order to identify a group of n ticketsEncipherment information $H_1$ which enciphered a result which connected number-of-sheets information which shows that it is the 1st ticketand was connected using a secret encryption key which only a vender knows as the 1st ticketMake it transmit to this consumer terminaland a ticket issuing means of the above-mentioned seller terminalNot operation mentioned above but a password transmitted from the above-mentioned consumer terminal and the issued banknotes newest ticket are receivedIf number-of-sheets information acquired as a result of decoding encipherment information $H_m$ ($1 <= m <= n$) which receivedand which is the issued banknotes newest ticket using a secret encryption key which

only a vender knows is number-of-sheets information which shows that it is the n-th ticketIf the issue of banknotes of n tickets is completed and that is not righta received password and encipherment information $H_m$ (1 <=m<=n) which received and which is the issued banknotes newest ticketsUID obtained as a result of decoding using a secret encryption key which only a vender knowsIt may be made to transmit encipherment information $H_{m+1}$ which enciphered a result which connected number-of-sheets information which shows that they are the m+1st ticketsand was connected using a secret encryption key which only a vender knows to this consumer terminal as a following ticket.

[0027]

[Embodiment of the Invention]Hereafteran embodiment of the invention is described with reference to drawings.

[0028]In the drawing referred to by the following explanationthe same numerals shall express the same component. Therebythis invention is not limited.

[0029](A 1st embodiment) A 1st embodiment of this invention is described first.

[0030]Drawing 1 is a figure showing the outline composition of the electronic coupon system concerning a 1st embodiment.

[0031]The electronic coupon system concerning a 1st embodimentAs it is a system which consumer $200_1$ - $200_n$ (it is also only hereafter called "the consumer 200".)and the vender 100 use and is shown in drawing 1Via the communications networks 300such as the Internetit is connected mutually and consumer terminal $201_1$ which is a terminal which the consumer 200 uses - $201_n$ (it is also only hereafter called "the consumer terminal 201".)and the seller terminal 101 which is terminals which the vender 100 uses are constituted.

[0032]In the electronic coupon system concerning a 1st embodimentBecause the consumer 200 exchanges data between the seller terminals 101 via the communications network 300 using the consumer terminal 201. The issue of banknotes of a coupon can be required of the vender 100or it enables it to require use of the coupon issued by the vender 100. At this timeusing the seller terminal 101a coupon is issued to the consumer 200 or the vender 100 verifies the coupon used by the consumer 200.

[0033]In the electronic coupon system especially built over a 1st embodimentIt also enables it to require use of a coupon of the vender 100 directly because the consumer 200 prints the coupon issued by the vender 100 and brings the printed coupon in a store using the consumer terminal 201. At this timethe vender 100 verifies the coupon which the consumer 200 brought using the seller terminal 101.

[0034]Namelythe electronic coupon system concerning a 1st embodimentElectronic-commerce-technology environment performed via the communications network 300 is realizedand the consumer 200 enables it to use the coupon issued by the vender 100 not only in the virtual store established on the communications network 300 but in the store which exists actually.

[0035]Nextthe hardware constitutions of the seller terminal 101 and the consumer terminal 201 which constitute the electronic coupon system concerning a 1st embodiment are explained using drawing 2 and drawing 3.

[0036]Drawing 2 is a figure showing the hardware constitutions of the seller terminal 101.
[0037]As shown in drawing 2the seller terminal 101 has the composition that the communication interface 102the display 103the input device 104the memory storage 105the central processing unit (CPU) 106and the temporary memory (memory) 107 of each other were connected by bus 110.
[0038]The communication interface 102 is an interface for exchanging data between the consumer terminals 201 via the communications network 300.
[0039]The display 103 is used in order to display the message to the vender 100 using the seller terminal 101etc.and it comprises CRTa liquid crystal displayetc.
[0040]The input device 104 is used in order that the vender 100 using the seller terminal 101 may input dataa commandetc.and it comprises a keyboarda mouseetc.
[0041]The memory storage 105 is used in order to memorize permanently the program and data which are used with the seller terminal 101and it comprises a hard diska floppy disketc.
[0042]CPU106 controls the component of the seller terminal 101 in generalizationor performs various data processing.
[0043]The operating system ("OS" is called hereafter.) 107athe program which CPU106such as the coupon issue of banknotes and the verification processing program 107bexecuteetc. are temporarily stored in the memory 107.
[0044]HereOS107a is a program for realizing functionssuch as file managementprocess controland device managementin order to control the seller terminal 101 whole. The coupon issue of banknotes and the verification processing program 107b are programs for issuing a coupon to the consumer 200 or verifying the coupon in which use was demanded from the consumer 200.
[0045]Drawing 3 is a figure showing the hardware constitutions of the consumer terminal 201.
[0046]As shown in drawing 3the consumer terminal 201 The communication interface 202The display 203the input device 204the memory storage 205the central processing unit (CPU) 206the temporary memory (memory) 207and the printer 208 have composition mutually connected by bus 210.
[0047]The communication interface 202 is an interface for exchanging data between the seller terminals 101 via the communications network 300.
[0048]The display 203 is used in order to display the message to the consumer 200 using the consumer terminal 201etc.and it comprises CRTa liquid crystal displayetc.
[0049]The input device 204 is used in order that the consumer 200 using the consumer terminal 201 may input dataa commandetc.and it comprises a keyboarda mouseetc.
[0050]The memory storage 205 is used in order to memorize permanently the program and data which are used with the consumer terminal 201and it comprises a hard diska floppy disketc.
[0051]CPU206 controls the component of the consumer terminal 201 in generalizationor performs various data processing.

[0052]OS207athe program which CPU206such as a coupon demandreceptionand the calling processing program 207bexecuteetc. are temporarily stored in the memory 207.
[0053]HereOS207a is a program for realizing functionssuch as file managementprocess controland device managementin order to control the consumer terminal 201 whole. A coupon demandreceptionand the calling processing program 207b are programs for requiring the issue of banknotes of a coupon of the vender 100receiving the coupon issued by the vender 100or requiring use of a coupon of the vender 100.
[0054]The printer 208 is used in order to print electronic dataand it comprises a printer etc.
[0055]Nextoperation of the electronic coupon system concerning a 1st embodiment is explained.
[0056]following explanation **** -- the consumer terminal 201 performs actually processing which the consumer 200 performs with the consumer's 200 directionsand the seller terminal 101 performs actually processing which the vender 100 performs with the vender's 100 directions.
[0057]Drawing 4 is a figure for explaining operation until the consumer 200 receives the coupon which required the issue of banknotes of the coupon of the vender 100and was issued by the vender 100.
[0058]In drawing 4the consumer 200 assumes first that the conditions which receive the issue of banknotes of a coupon from the vender 100 are fulfilled (S2000).
[0059]The consumer 200 performs the coupon request process (S2400) mentioned laterand transmits the password 501 of the enciphered self to the vender 100.
[0060]If the password 501 is receivedthe vender 100 will perform coupon ticket issue processing (S1300) mentioned laterand will transmit the coupon 502 and the digital signature 503 of the coupon 502 to the consumer 200.
[0061]If the coupon 502 and the digital signature 503 are receivedthe consumer 200 will perform coupon reception (S2500) mentioned laterand will keep the received coupon 502.
[0062]Drawing 5 is a figure for explaining operation until the consumer 200 who has already received the issue of banknotes of the coupon uses a coupon via the communications network 300 and the vender 100 verifies a coupon.
[0063]In drawing 5the consumer 200 who has already received the issue of banknotes of the coupon performs coupon use on-line processing (S2600) mentioned laterand transmits the coupon 502 which came to hand by coupon reception (S2500)and the password 501 of the enciphered self to the vender 100.
[0064]If the coupon 502 and the password 501 are receivedthe vender 100 will perform coupon verification processing (S1400) mentioned laterand will verify the received coupon 502.
[0065]Drawing 6 is a figure for explaining operation until the consumer 200 who has already received the issue of banknotes of the coupon prints a couponand brings and uses the printed coupon for a store and the vender 100 verifies a

coupon.
[0066]In drawing 6the consumer 200 who has already received the issue of banknotes of the coupon performs coupon use off-line processing (S2700) mentioned laterand brings the printed coupon 504 in a store.
[0067]Coupon verification processing (S1400) will be performed and the vender 100 will verify the received coupon 504if the coupon 504 which the consumer 200 brought is received.
[0068]Drawing 7 is a processing flow chart of the coupon request process (S2400) of drawing 4and this processing is realized by a coupon demandreceptionand the calling processing program 207b.
[0069]As shown in drawing 7in a coupon request process (S2400)firstto the vender 100the consumer 200 demands the vender's 100 public key in a public-key crypto systemand receives a public key (Step 2401).
[0070]Thenthe consumer 200 enters the password which only self knows (Step 2402).
[0071]Thenthe consumer 200 enciphers the password entered at Step 2402 using the public key which came to hand at Step 2401 (Step 2403)and transmits the enciphered password 501 to the vender 100 (Step 2404).
[0072]Drawing 8 is a processing flow chart of the coupon ticket issue processing (S1300) of drawing 4and this processing is realized by the coupon issue of banknotes and the verification processing program 107b.
[0073]As shown in drawing 8in coupon ticket issue processing (S1300) the vender 100Firstreception of the enciphered password 501 will decode the received password 501 using the vender's 100 secret key in a public-key crypto system (Step 1302). (Step 1301) Although here shows the example which enciphers a password using public-key-encryption artif it is not intercepted when a password passes the communications network 300what kind of encoding technology may be used.
[0074]Thenthe vender 100 performs irreversible transformation to the password 501 decoded at Step 1302 (Step 1303). Hereafterthe result of having performed irreversible transformation to the password is called the irreversible transformation value or PH of a password.
[0075]Thenthe vender 100 sets up the coupon information about effect of a couponsuch as worth (for exampleamount of money) of a serial numberthe term of validityand a coupon (Step 1304)and the digital signature of the set-up coupon information is calculated using the vender's 100 secret key (Step 1305). And the irreversible transformation value calculated at Step 1303the coupon information set up at Step 1304and the digital signature calculated at Step 1305The coupon 502 as a document is created by creating the coupon indicated as data (for examplea numbera characteretc.) which can be viewed (Step 1306).
[0076]Thenthe coupon 502 which the vender 100 calculated the digital signature 503 of the coupon 502 whole as a document using the vender's 100 secret key (Step 1307)and was created at Step 1306The digital signature 503 calculated at Step 1307 is transmitted to the consumer 200 (Step 1308).

[0077]Drawing 9 is a processing flow chart of the coupon reception (S2500) of drawing 4and this processing is realized by a coupon demandreceptionand the calling processing program 207b.
[0078]As shown in drawing 9in coupon reception (S2500) the consumer 200By verifying the digital signature 503 which receivedif the coupon 502 and the digital signature 503 which the vender 100 transmitted are received (Step 2501). It is verified whether the received coupon 502 is altered while being transmitted via the communications network 300 (Step 2502). In Step 2502in detailthe consumer 200 will judge that the received coupon 502 is not alteredif the received coupon 502 is compared with the result of having decoded the digital signature 503 which received using the vender's 100 public key and both are in agreement.
[0079]And if not alteredthe received coupon 502 is saved at the memory storage 205 (Step 2503).
[0080]Hereas for the coupon 502it is preferred to be able to consider it as form as shown in drawing 14 for exampleand to make it displayed on the display 203 at the time of reception.
[0081]Drawing 10 is a processing flow chart of coupon use on-line processing (S2600) of drawing 5and this processing is realized by a coupon demandreceptionand the calling processing program 207b.
[0082]As shown in drawing 10in coupon use on-line processing (S2600)firstto the vender 100the consumer 200 demands the vender's 100 public keyand receives a public key (Step 2601).
[0083]Thenthe consumer 200 enters the password (the same password as the password entered by the coupon request process (S2400)) which knows only self (Step 2602).
[0084]Thenthe password 501 which the consumer 200 enciphered the password entered at Step 2602 using the public key which came to hand at Step 2601 (Step 2603)and was encipheredThe coupon 502 which came to hand by the coupon reception (S2500) shown in drawing 9 is transmitted to the vender 100 (Step 2604).
[0085]Drawing 11 is a processing flow chart of coupon use off-line processing (S2700) of drawing 6and this processing is realized by a coupon demandreceptionand the calling processing program 207b.
[0086]As shown in drawing 11in coupon use off-line processing (S2700)the consumer 200 prints the coupon 502 which came to hand by the coupon reception (S2500) shown in drawing 9 with the printer 208 (Step 2701).
[0087]Herethe forms of the printed coupon 504 are the form of the coupon 502 shown in drawing 14and the same form.
[0088]Thenthe consumer 200 brings the printed coupon 504 in a storeand tells the vender 100 the password (the same password as the password entered by the coupon request process (S2400)) which only self knows (Step 2702). Step 2702 is action which consumer 200 self performsand is not performed with the consumer terminal 201.
[0089]Drawing 12 is a processing flow chart of drawing 5 and the coupon verification processing (S1400) of drawing 6and this processing is realized by the

coupon issue of banknotes and the verification processing program 107b.
[0090]As shown in drawing 12coupon verification processing (S1400). [ whether the coupon used is the coupon 502 which arrived on-line via the communications network 300and ] Or processing is divided by whether it is the coupon (printed coupon) 504 brought directly (Step 1401).
[0091]In being the coupon 504 brought directlythe vender 100 starts processing from the document verification processing of Step 1404. Howeveralthough it is necessary to acquire the variety of information the vender 100 is indicated to be on the coupon 504 at this timeabout an acquisition methodit is arbitrary.
[0092]In being the coupon 502 which arrived on-line via the communications network 300With this coupon 502the vender 100 receives the enciphered password 501 (Step 1402)and decodes the received password 501 using the vender's 100 secret key (Step 1403).
[0093]In Step 1404the vender 100 performs document verification processing which verifies the variety of information indicated on the coupon. The details of document verification processing are mentioned later.
[0094]When the verification about all the information is passed as a result of the document verification processing of Step 1404in order to prevent double use of (Step 1405) and a couponThe serial number in the coupon information indicated on the coupon is registered into a used serial list of number (Step 1406)and effect that the coupon was defined is demonstrated (Step 1407). When at least one is a rejection(Step 1405) and error handling are performed (Step 1408).
[0095]Drawing 13 is a processing flow chart of the document verification processing (Step 1404) of drawing 12.
[0096]As shown in drawing 13in document verification processing (Step 1404)the vender 100 calculates first the digital signature of the coupon information indicated on the coupon as a document using the vender's 100 secret key (Step 1410).
[0097]And since the coupon is altered if verification is not passed (i.e.if the calculated digital signature and the digital signature indicated on the coupon are not in agreement) (Step 1411)error handling is performed (Step 1417).
[0098]If verification is passed (i.e.if the calculated digital signature and the digital signature indicated on the coupon are in agreement) (Step 1411)The irreversible transformation value of the password (or password told by the consumer 200) obtained at Step 1403 is calculatedand is compared with the calculated irreversible transformation value and the irreversible transformation value indicated on the coupon as a document (Step 1412).
[0099]Since it is thought that it is the unauthorized use of the coupon by the third party who does not know the password at the time of the coupon issue of banknotes if both are not in agreement as a result of comparison of Step 1412 (Step 1413)error handling is performed (Step 1418).
[0100]The vender 100 verifies whether the serial number in the coupon information indicated on the coupon as a document is registered into the used serial list of number (Step 1414). If already registered (Step 1415)error handling

will be performed for the reason of double use of a coupon (Step 1419).
[0101]Finallythe vender 100 verifies whether it is a coupon within the term of validity with reference to the term of validity in the coupon information indicated on the coupon as a document (Step 1416)and if he is outside the term of validityhe will perform error handling of a term-of-validity piece (Step 1420).
[0102]If all verification of these is passedit becomes effective [ a coupon ] and effect will be demonstrated.
[0103]In the electronic coupon system built over a 1st embodiment as explained aboveIf a serial numberthe term of validitythe amount of moneyetc. are alteredhe calculates using the secret key which is the information to which only the vender 100 knows the troubled digital signature of coupon informationand is trying to create the coupon which indicated the calculated digital signature as data which can be viewed.
[0104]Thereforeaccording to the electronic coupon system concerning a 1st embodimenteven when the consumer 200 prints and uses an electronic couponforgery and an alteration of a coupon can be detected by verifying the digital signature indicated on the printed coupon.
[0105]He is trying to create the coupon which indicated the irreversible transformation value of the password which the consumer 200 presented as data which can be viewed in the electronic coupon system concerning a 1st embodiment at the time of the issue of banknotes of a coupon. He is trying to compare the irreversible transformation value of the password which showed the vender 100 the password which only the consumer 200 who demanded the issue of banknotes knowsand the consumer 200 presented with the irreversible transformation value indicated on the coupon at the time of use of a coupon.
[0106]Thereforeaccording to the electronic coupon system concerning a 1st embodimenteven if a coupon is stolenthe third party who does not know the password which the issue-of-banknotes demand of the coupon was shown can be prevented from using a coupon improperly.
[0107]Although the example which indicated on the coupon the digital signature calculated using the vender's 100 secret key in a public-key crypto system about coupon information in the electronic coupon system concerning a 1st embodiment as data which can be viewed is shownThe encipherment information enciphered using the secret encryption key which only the vender 100 knows is indicated on a coupon as data which can be viewedand it may be made to verify this encipherment information.
[0108]In the electronic coupon system concerning a 1st embodimentSince it is convenient even if the example which indicated about the password the irreversible transformation value which performed irreversible transformation on the coupon as data which can be viewed is shownand it exhibits the irreversible transformation method according to this exampleWhen the irreversible transformation value of a password is inharmoniousthe consumer 200 is able to calculate and check the irreversible transformation value of the password which self presented. Howeverthe encipherment information enciphered with the

encryption method which can encipher only the vender 100 is indicated on a coupon about a password as data which can be viewedand it may be made to verify this encipherment information.

[0109]This invention is not limited to a 1st embodiment mentioned aboveand various modification is possible for it within the limits of the gist.

[0110]For examplein the electronic coupon system concerning a 1st embodimentwhen transmitting a password to the vender 100the consumer 200 acquires the vender's 100 public keyand is made to perform encryption communicationbut he does not limit this invention to this. The consumer 200 can use the public key after 2 timesif the vender's 100 public key comes to hand once. As long as it can have a common key between the vender 100 and the consumer 200it may be made to encipher using secret key cryptosystem art.

[0111]When transmitting a password from the consumer 200 to the vender 100 in the electronic coupon system concerning a 1st embodimentin order that the enciphered password may prevent it being stolen as it is and used improperlyA password is enciphered with other information (a random number and a suitable number may be sufficient.)and it may be made to transmit.

[0112]In the electronic coupon system concerning a 1st embodimentalthough he is made to indicate a digital signature on a coupon as data of a numerical valuea characteretc. which can be viewedif viewing after printing is possible for the vender 100he needs a bar code etc.for example. If it indicates as a bar codewhen the vender 100 acquires a variety of information from the printed couponhe can use a bar code reader.

[0113]In the electronic coupon system concerning a 1st embodimentalthough the vender 100 is made to indicate independently the irreversible transformation value of the consumer's 200 passwordand the digital signature of coupon informationsuch as a serial numberthe term of validityand the amount of moneyon a couponIt may be made for a password to also calculate a digital signature together with coupon information. After the information on the origin which calculates digital signaturessuch as coupon information and a passwordat this time performs irreversible transformationit may be made to calculate a digital signature.

[0114]In (a 2nd embodiment) and timea coupon has what demonstrates effect by one sheetand a thing which demonstrates effect only when a certain kind of conditions are fulfilled by the vender's 100 sales policy. For examplewhen only the number of sheets defined beforehand is collectedonly a different point from a 1st embodiment that mentioned above the case where a coupon (this kind of coupon is hereafter called a "ticket" especially.) which demonstrates effect was dealt withas a 2nd embodiment is explained.

[0115]The outline composition of the electronic coupon system concerning a 2nd embodiment is the same as the outline composition shown in drawing 1.

[0116]Drawing 15 is a figure showing the hardware constitutions of the seller terminal 101.

[0117]A different point from the hardware constitutions shown in drawing 2 is a point that the ticket issue of banknotes and the verification processing program

107c are temporarily stored in the memory 107.
[0118]The ticket issue of banknotes and the verification processing program 107c are programs for issuing a ticket to the consumer 200 or verifying the ticket in which use was demanded from the consumer 200.
[0119]Drawing 16 is a figure showing the hardware constitutions of the consumer terminal 201.
[0120]A different point from the hardware constitutions shown in drawing 3 is a point that a ticket demandreceptionand the calling processing program 207c are temporarily stored in the memory 207.
[0121]A ticket demandreceptionand the calling processing program 207c are programs for requiring the issue of banknotes of a ticket of the vender 100receiving the ticket issued by the vender 100or requiring use of a ticket of the vender 100.
[0122]Nextoperation of the electronic coupon system concerning a 2nd embodiment is explained.
[0123]The consumer terminal 201 performs actually processing which the consumer 200 performs with the consumer's 200 directions like a 1st embodiment that also mentioned following explanation **** aboveand the seller terminal 101 performs actually processing which the vender 100 performs with the vender's 100 directions.
[0124]Drawing 17 is a figure for explaining operation until the consumer 200 receives the 1st ticket that required the issue of banknotes of the 1st ticket of the vender 100and was issued by the vender 100. Only n tickets shall demonstrate effectwhen it collects.
[0125]In drawing 17firstthe consumer 200 performs the initial ticket issue-of-banknotes request process (S2100) mentioned laterand transmits the password 501 of the enciphered self to the vender 100.
[0126]The peculiar value ("UID" is called hereafter.) 505 given in order that the vender 100 might perform initial ticket ticket issue processing (S1100) mentioned later and might identify the group of n ticketsif the password 501 was receivedAlthough the secret information (for examplethe vender's 100 secret key) which only the password 501 and UID505 which receivedand the vender 100 know was connectedn-th irreversible transformation value $H_n$ (506 $_n$) is transmitted to the consumer 200 as the 1st ticket.
[0127]If UID505 and $H_n$ (506 $_n$) are receivedthe consumer 200 will perform ticket reception (S2200) mentioned laterand will keep UID505 and $H_n$ (506 $_n$) which received.
[0128]Drawing 18 is a figure for explaining operation until the consumer 200 receives the ticket after the 2nd sheet that required the issue of banknotes of the ticket after the 2nd sheet of the vender 100and was issued by the vender 100.
[0129]In drawing 18firstwhen receiving the issue of banknotes of the 2nd ticketthe consumer 200The ticket issue-of-banknotes request process (S2300) mentioned later is performedand the password 501 of the enciphered selfand UID505 and $H_n$ (506 $_n$) which came to hand by the ticket reception (S2200) of the 1st sheet are

transmitted to the vender 100.
[0130]If the vender 100 receives the password 501UID505and $H_n$ (506 $_n$)The password 501 and UID505 which performed ticket ticket issue processing (S1200) mentioned laterand receivedand $H_n$ (506 $_n$)From the vender's 100 secret key$H_{n-1}$ (506 $_{n-1}$) is calculated and calculated $H_{n-1}$ (506 $_{n-1}$) is transmitted to the consumer 200 as the 2nd ticket.
[0131]Ticket reception (S2200) will be performed and the consumer 200 will keep $H_{n-1}$ (506 $_{n-1}$) which receivedif $H_{n-1}$ (506 $_{n-1}$) is received.
[0132]Similarlywhen receiving the issue of banknotes of the m+1st (1 <=m<n) ticketsthe consumer 200A ticket issue-of-banknotes request process (S2300) is performedand the password 501 of the enciphered selfand UID505 and $H_{n-(m-1)}$ ($506_{n-(m-1)}$) which came to hand by the ticket reception (S2200) of the m-th sheet are transmitted to the vender 100.
[0133]If the vender 100 receives the password 501UID505and $H_{n-(m-1)}$ ($506_{n-(m-1)}$)The password 501 and UID505 which performed ticket ticket issue processing (S1200)and receivedand $H_{n-(m-1)}$ ($506_{n-(m-1)}$)From the vender's 100 secret key$H_{n-m}$ (506 $_{n-m}$) is calculated and calculated $H_{n-m}$ (506 $_{n-m}$) is transmitted to the consumer 200 as the m+1st tickets.
[0134]Ticket reception (S2200) will be performed and the consumer 200 will keep $H_{n-m}$ (506 $_{n-m}$) which receivedif $H_{n-m}$ (506 $_{n-m}$) is received.
[0135]Thusfor the consumer 200 to be able to collect n tickets and demonstrate the effect of these n tickets. A ticket issue-of-banknotes request process (S2300) is performedand the password 501 of the enciphered selfand UID505 and $H_1$ (506 $_1$) which came to hand by the ticket reception (S2200) of the n-th sheet are transmitted to the vender 100.
[0136]If the vender 100 receives the password 501UID505and $H_1$ (506 $_1$)Ticket ticket issue processing (S1200) is performedand from the password 501 and UID505 which received$H_1$ (506 $_1$)and the vender's 100 secret keythe consumer 200 checks having collected tickets and performs only n n ticket collection end processing (S1250).
[0137]Drawing 19 is a processing flow chart of the initial ticket issue-of-banknotes request process (S2100) of drawing 17and this processing is realized by a ticket demandreceptionand the calling processing program 207c.
[0138]As shown in drawing 19in an initial ticket issue-of-banknotes request process (S2100)firstto the vender 100the consumer 200 demands the vender's 100 public keyand receives a public key (Step 2101).
[0139]Thenthe consumer 200 enters the password which only self knows (Step 2102).
[0140]Thenthe consumer 200 enciphers the password entered at Step 2102 using the public key which came to hand at Step 2101 (Step 2103)and transmits the enciphered password 501 to the vender 100 (Step 2104).
[0141]Drawing 20 is a processing flow chart of the initial ticket ticket issue processing (S1100) of drawing 17and this processing is realized by the ticket issue of banknotes and the verification processing program 107c.

[0142]If the vender 100 receives the enciphered password 501 first in initial ticket ticket issue processing (S1100) as shown in drawing 20 (Step 1101)the received password 501 will be decoded using the vender's 100 secret key (Step 1102). Although here shows the example which enciphers a password using public-key-encryption artif it is not intercepted when a password passes the communications network 300what kind of encoding technology may be used.
[0143]Thenthe vender 100 creates UID505 which is a peculiar value for identifying the group of n tickets (Step 1103)Irreversible transformation is performed to the password decoded at Step 1102UID505 which were created at Step 1103and the thing which combined the vender's 100 secret key (Step 1104). Although the result of having performed irreversible transformation to what combined a passwordUIDand a secret key hereafter is called irreversible transformation value $H_m$ (1 <=m<=n)irreversible transformation value $H_m$ calculated at Step 1104 is $H_1$ (506 $_1$).
[0144]Thenthe vender 100 calculates irreversible transformation value $H_{i+1}$ (1 <=i<n) of $H_i$ (Step 1105). In Step 1105in detail the vender 100As shown in drawing 24irreversible transformation value $H_2$ (506 $_2$) of $H_1$ (506 $_1$) is calculated firstIrreversible transformation value $H_{i+1}$ (1 <=i<n) of $H_i$ is repeated and calculated until it calculates irreversible transformation value $H_n$ (506 $_n$) of $H_{n-1}$ (506 $_{n-1}$).
[0145]Finallythe vender 100 transmits UID505 created at Step 1103and n-th irreversible transformation value $H_n$ (506 $_n$) to the consumer 200 as the 1st ticket (Step 1106).
[0146]Drawing 21 is a processing flow chart of drawing 17 and the ticket reception (S2200) of drawing 18and this processing is realized by a ticket demandreceptionand the calling processing program 207c.
[0147]As shown in drawing 21in ticket reception (S2200) the consumer 200If the data transmitted by the vender 100 is received (Step 2201)it judges whether UID505 is contained in the received data (Step 2202)and when containedUID505 is saved at the memory storage 205 (Step 2203).
[0148]Finallythe consumer 200 saves irreversible transformation value $H_m$ which received at the memory storage 205 (Step 2204).
[0149]The consumer 200 can recognize the how many ticket was issued at counting the number of times which saved irreversible transformation value $H_m$ which received at the memory storage 205. Thenin the consumer terminal 201it is preferred that the display which shows the how many ticket was issued is made by the display 203.
[0150]Drawing 22 is a processing flow chart of the ticket issue-of-banknotes request process (S2300) of drawing 18and this processing is realized by a ticket demandreceptionand the calling processing program 207c.
[0151]As shown in drawing 22in a ticket issue-of-banknotes request process (S2300)firstto the vender 100the consumer 200 demands the vender's 100 public keyand receives a public key (Step 2301).
[0152]Thenthe consumer 200 enters the password (the same password as the password entered by the initial ticket issue-of-banknotes request process

(S2100)) which knows only self (Step 2302).
[0153]Thenthe password 501 which the consumer 200 enciphered the password entered at Step 2302 using the public key which came to hand at Step 2301 (Step 2303)and was encipheredUID505 which came to hand by the ticket reception (S2200) shown in drawing 21and irreversible transformation value $H_m$ which came to hand by ticket reception (S2200) 1 time ago are transmitted to the vender 100 (Step 2304).
[0154]Thusby transmitting irreversible transformation value $H_m$ which came to hand by ticket reception (S2200) 1 time ago the vender 100It can know now the how many newest tickets that issued banknotes to the consumer 200 there arei.e.is the consumer 200 collecting the tickets up to the how many sheets?.
[0155]The consumer 200 should demand the issue of banknotes of the 1st ticketor (should the initial ticket issue-of-banknotes request process (S2100) shown in drawing 19 be performed?). or -- or it should require the issue of banknotes of the ticket after the 2nd sheet (should the ticket issue-of-banknotes request process (S2300) shown in drawing 22 be performed?) -- ******** -- it can be judged whether UID505 is memorized by the memory storage 205.
[0156]Drawing 23 is a processing flow chart of the ticket ticket issue processing (S1200) of drawing 18and this processing is realized by the ticket issue of banknotes and the verification processing program 107c.
[0157]As shown in drawing 23in ticket ticket issue processing (S1200) the vender 100Firstreception of the enciphered password 501UID505and irreversible transformation value $H_m$ will decode the received password 501 using the vender's 100 secret key (Step 1202). (Step 1201) Although here shows the example which enciphers a password using public-key-encryption artif it is not intercepted when a password passes the communications network 300what kind of encoding technology may be used.
[0158]Thenalthough the vender 100 combined the secret key of UID505 and the vender 100 who received at the password decoded at Step 1202and Step 1201he calculates irreversible transformation value $H_1$ (Step 1203).
[0159]Thenthe vender 100 verifies whether $H_m$ which received at Step 1201and $H_1$ calculated at Step 1203 are in agreement (Step 1204)Since it means that the consumer 200 finished collecting n tickets when in agreementit progresses to Step 1208 and ticket collection completion processing is performed. The ticket collection completion processing of Step 1208 is equivalent to ticket collection end processing (S1250) of drawing 18and the contents of processing can consider various contents of processing according to the vender's 100 sales policyand it does not define them in particular.
[0160]When $H_m$ which received at Step 1201and $H_1$ calculated at Step 1203 are not in agreementthe vender 100 (Step 1204)Since it means that the consumer 200 has not finished collecting n ticketsirreversible transformation value $H_{i+1}$ ($1 <= i < n$) of $H_i$ is calculated (Step 1205)and it asks for i ($1 < i <= n$) used as $H_m = H_i$ (Step 1206). In Step 1206like Step 1105 of the initial ticket ticket issue processing (S1100) shown in drawing 20although the vender 100 repeats and calculates irreversible

transformation value $H_{i+1}$ (1 <=i<n) of $H_i$Calculation can be stopped when i (1<i<=n) used as $H_m=H_i$ is able to be found.

[0161]Heresince it means that either is unjust at least of the password 501 and UID505 which received at Step 1201and Hm when i used as $H_m=H_i$ does not existerror handling is performed (Step 1209).

[0162]The vender 100 transmits $H_{i-1}$ to the consumer 200 with UID505when i used as $H_m=H_i$ exists (Step 1207).

[0163]In the electronic coupon system built over a 2nd embodiment as explained aboveFrom what connected UID for identifying the group of the secret key of the vender 100 who is the secret information which only the vender 100 knowsthe password which is the information which only the consumer 200 knowsand n tickets at the time of the issue of banknotes of a ticket. Repeatcalculate an irreversible transformation value and in n-th irreversible transformation value $H_n$the n-1st irreversible transformation value $H_{n-1}$--the turn of 2nd irreversible transformation value $H_2$ and 1st irreversible transformation value $H_1$. He is trying to reply each irreversible transformation value to the consumer 200. He is trying to transmit $H_m$ and UID which were transmitted from the consumer 200 1 time ago to the vender 100and a password. The data required to calculate an irreversible transformation value for every consumer 200 is made to be transmitted from the consumer 200 to the vender 100.

[0164]Thereforeeven if a ticket is stolen [ according to the electronic coupon system concerning a 2nd embodiment ] on a channel in addition to the effect by a 1st embodiment mentioned aboveThe third party who does not know a password can be prevented from using a ticket improperlyand it becomes unnecessary to manage how many tickets were already issued every consumer 200 by the vender 100 side.

[0165]Also in the electronic coupon system concerning a 2nd embodimentas a 1st embodiment mentioned above explainedvarious modification is possible within the limits of the gist of this invention.

[0166]For examplein the electronic coupon system concerning a 2nd embodimentalthough the vender 100 is made to calculate an irreversible transformation value by using the vender's 100 secret key at the time of the ticket issue of banknotesSince this calculation is good if incalculable except vender 100if the algorithm of irreversible transformation is disclosureit is not necessary to use the vender's 100 secret key.

[0167]In the electronic coupon system concerning a 2nd embodimentAlthough the vender 100 transmits UID to the consumer 200 at the time of the initial ticket issue of banknotesand the consumer 200 keeps the UID and is made to transmit kept UID from the consumer 200 to the vender 100 after thatIt may be made to transmit UID from the vender 100 to the consumer 200 each time at the time of the ticket issue of banknotes.

[0168]Although the vender 100 is made to reply the irreversible transformation value calculated from the vender's 100 secret keythe passwordand the thing that connected UID at the time of the ticket issue of banknotes to the consumer 200

in the electronic coupon system concerning a 2nd embodimentWhat connected a password and UID is enciphered using the secret encryption key (for examplethe vender's 100 secret key in a public-key crypto system) which only the vender 100 knowsand it may be made to reply the enciphered encipherment information to the consumer 200. The vender 100 in detail based on encipherment information $H_1$ of what connected a password and UIDEncipherment information $H_{i+1}$ of encipherment information $H_i$ ($1 <= i < n$) is calculated one by oneIt may be made to reply each encipherment information to the consumer 200 in n-th encipherment information $H_n$the n-1st encipherment information $H_{n-1}$--the turn of 2nd encipherment information $H_2$ and 1st encipherment information $H_1$.

[0169]Although the vender 100 is made to reply the irreversible transformation value calculated from the vender's 100 secret keythe passwordand the thing that connected UID at the time of the ticket issue of banknotes to the consumer 200 in the electronic coupon system concerning a 2nd embodimentWhat connected the number-of-sheets information which shows a passwordUIDand the how many ticket it isIt enciphers using the secret encryption key (for examplethe vender's 100 secret key in a public-key crypto system) which only the vender 100 knowsand may be made to reply the enciphered encipherment information to the consumer 200. If it does in this waythe vender 100 can know how many tickets the consumer 200 collected using the number-of-sheets information acquired as a result of decoding the encipherment information transmitted to the issue-of-banknotes demand of a ticket using the secret encryption key which only the vender 100 knows from the consumer 200.

[0170]In the electronic coupon system concerning a 2nd embodimentalthough the vender 100 is made to transmit an irreversible transformation value to the consumer 200 at the time of the ticket issue of banknotesThe ticket indicated as data which can view an irreversible transformation value as well as the coupon explained by a 1st embodiment mentioned above is createdand it may be made to transmit the ticket as a document to the consumer 200. If it does in this wayin the consumer terminal 201for examplea display as shown in drawing 25 is made by the display 203and it can be shown the how many ticket was issued.

[0171]Like the coupon explained by a 1st embodiment mentioned above also in the electronic coupon system concerning a 2nd embodimentfrom the vender 100 to the consumer 200 with a ticket. If the digital signature of the whole ticket may be made to be transmitted and it does in this wayit is verifiable whether the received ticket is altered by the consumer 200 side who received the issue of banknotes of the ticket.

[0172](A 3rd embodiment) and the issue-of-banknotes person for exclusive use whom the vender 100 prepared the issue of banknotes of the coupon independently in time may be made to carry outand only a different point from a 1st embodiment that mentioned above the case where the issue-of-banknotes person of a coupon was providedas a 3rd embodiment is explained hereafter.

[0173]Drawing 26 is a figure showing the outline composition of the electronic coupon system concerning a 3rd embodiment.

[0174]The electronic coupon system concerning a 3rd embodimentConsumer $200_1$ – $200_n$ (it is also only hereafter called "the consumer 200".)As it is a system which seller terminal $600_1$ – $600_n$ (it is also only hereafter called "the vender 600".)and the issue-of-banknotes person 700 use and is shown in drawing 26Consumer terminal $201_1$ which is a terminal which the consumer 200 uses – $201_n$ (it is also only hereafter called "the consumer terminal 201".)Via the communications networks 300such as the Internetit is connected mutually and seller terminal $601_1$ which is a terminal which the vender 600 uses – $601_n$ (it is also only hereafter called "the seller terminal 601".)and the issue-of-banknotes person terminal 701 which is terminals which the issue-of-banknotes person 700 uses are constituted.

[0175]Nextthe hardware constitutions of the issue-of-banknotes person terminal 701 which constitutes the electronic coupon system concerning a 3rd embodimentand the store terminal 601 are explained using drawing 27 and drawing 28. The hardware constitutions of the consumer terminal 201 are the same as the hardware constitutions shown in drawing 3.

[0176]Drawing 27 is a figure showing the hardware constitutions of the issue-of-banknotes person terminal 701.

[0177]As shown in drawing 27the issue-of-banknotes person terminal 701 The communication interface 702The display 703the input device 704the memory storage 705the central processing unit (CPU) 706and the temporary memory (memory) 707 have composition connected mutually by bus 710andfundamentallyit is the same as that of the hardware constitutions of the seller terminal 101 shown in drawing 2.

[0178]OS707athe program which CPU706such as the coupon issue of banknotes and the verification processing program 707bexecuteetc. are temporarily stored in the memory 707.

[0179]HereOS707a is a program for realizing functionssuch as file managementprocess controland device managementin order to control the issue-of-banknotes person terminal 701 whole. The coupon issue of banknotes and the verification processing program 707b are programs for issuing a coupon to the consumer 200 or verifying the coupon in which verification (it is verification about double use of a coupon as mentioned later.) was demanded from the vender 600.

[0180]Drawing 28 is a figure showing the hardware constitutions of the seller terminal 601.

[0181]A different point from the hardware constitutions shown in drawing 2 is a point that the coupon verification processing program 607b is temporarily stored in the memory 107 instead of the coupon issue of banknotes and the verification processing program 107b.

[0182]The coupon verification processing program 607b is a program for verifying the coupon in which use was demanded from the consumer 200.

[0183]Nextoperation of the electronic coupon system concerning a 3rd embodiment is explained.

[0184]The processing which the consumer 200 performs like a 1st embodiment

that also mentioned following explanation **** aboveThe processing which the consumer terminal 201 performs and the vender 600 performs with the consumer's 200 directions actuallyThe issue-of-banknotes person terminal 701 performs actually processing which the seller terminal 601 performs and the issue-of-banknotes person 700 performs further with the vender's 600 directions actually with the issue-of-banknotes person's 700 directions.

[0185]Drawing 29 is a figure for explaining operation until the consumer 200 receives the coupon which required the issue of banknotes of the coupon of the issue-of-banknotes person 700and was issued by the issue-of-banknotes person 700.

[0186]In drawing 29the consumer 200 assumes first that the conditions which receive the issue of banknotes of a coupon from the issue-of-banknotes person 700 are fulfilled (S2000).

[0187]The consumer 200 performs the coupon request process (S12400) mentioned laterand transmits the password 501 of the enciphered self to the issue-of-banknotes person 700.

[0188]If the password 501 is receivedthe issue-of-banknotes person 700 will perform coupon ticket issue processing (S7300) mentioned laterand will transmit the coupon 502 and the digital signature 503 of the coupon 502 to the consumer 200.

[0189]If the coupon 502 and the digital signature 503 are receivedthe consumer 200 will perform coupon reception (S12500) mentioned laterand will keep the received coupon 502.

[0190]It differs in that the vender 100 has replaced with the issue-of-banknotes person 700 the operation shown in drawing 29 in the operation shown in drawing 4.

[0191]Namelyalthough the processing flow chart of the coupon request process (S12400) of drawing 29 is the same as the processing flow chart of the coupon request process (S2400) shown in drawing 7The point of using the public key of the issue-of-banknotes person 700 instead of the vender's 100 public key differs from the point that the transmission destination of the enciphered password 501 becomes the issue-of-banknotes person 700 instead of the vender 100.

[0192]Although the processing flow chart of the coupon ticket issue processing (S7300) of drawing 29 is the same as the processing flow chart of the coupon ticket issue processing (S1300) shown in drawing 8The point (point that this processing is realized by the coupon issue of banknotes and the verification processing program 707b) that the issue-of-banknotes person 700 performs this processing differs from the point of using the secret key of the issue-of-banknotes person 700 instead of the vender's 100 secret key.

[0193]The processing flow chart of the coupon reception (S12500) of drawing 29 is the same as the processing flow chart of the coupon reception (S2500) shown in drawing 9.

[0194]Drawing 30 is a figure for explaining operation until the consumer 200 who has already received the issue of banknotes of the coupon uses a coupon via the communications network 300 and the vender 600 verifies a coupon.

[0195]In drawing 30the consumer 200 who has already received the issue of banknotes of the coupon performs coupon use on-line processing (S2600)and transmits the coupon 502 which came to hand by coupon reception (S12500)and the password 501 of the enciphered self to the vender 600.
[0196]If the coupon 502 and the password 501 are receivedthe vender 600 will perform coupon verification processing (S6400) mentioned laterand will verify the received coupon 502.
[0197]Drawing 31 is a figure for explaining operation until the consumer 200 who has already received the issue of banknotes of the coupon prints a couponand brings and uses the printed coupon for a store and the vender 600 verifies a coupon.
[0198]In drawing 31the consumer 200 who has already received the issue of banknotes of the coupon performs coupon use off-line processing (S2700)and brings the printed coupon 504 in a store.
[0199]If the coupon 504 which the consumer 200 brought is receivedthe vender 600 will perform coupon verification processing (S6400) mentioned laterand will verify the received coupon 504.
[0200]Respectivelyin the operation shown in drawing 5 and drawing 6the operation shown in drawing 30 and drawing 31 differs only in the contents of processing of the coupon verification processing (S6400) which the vender 600 performsand the contents of processing of this processing are later mentioned for it.
[0201]That isthe processing flow chart of coupon use on-line processing (S2600) of drawing 30 is the same as the processing flow chart of coupon use on-line processing (S2600) shown in drawing 10.
[0202]The processing flow chart of coupon use off-line processing (S2700) of drawing 31 is the same as the processing flow chart of coupon use off-line processing (S2700) shown in drawing 11.
[0203]Drawing 32 is a processing flow chart of drawing 30 and the coupon verification processing (S6400) of drawing 31and this processing is realized by the coupon verification processing program 607b.
[0204]As shown in drawing 32in coupon verification processing (S6400)the vender 600 performs coupon verification processing (S1200) shown in drawing 12and same processingbut the contents of processing of the document verification processing of Step 11404 differ so that it may mention later.
[0205]The vender 600 does not manage a used serial list of numberbut it is Step 11406The serial number indicated on the coupon is notified to the issue-of-banknotes person 700and it differs in trying that I have a serial number to a used serial list of number registered into the issue-of-banknotes person 700.
[0206]Drawing 33 is a processing flow chart of the document verification processing (Step 11404) of drawing 32.
[0207]As shown in drawing 33in document verification processing (Step 11404)the vender 600 performs document verification processing shown in drawing 13and same processingbut. At the point which has decoded the digital signature indicated on the coupon at Step 11410 using the public key of the issue-of-banknotes

person 700and Step 11414. The serial number indicated on the coupon is notified to the issue-of-banknotes person 700and it differs in trying that it is asked to the issue-of-banknotes person 700 whether the serial number is registered into the used serial list of number. Thenthe vender 600 will compare the result decoded at Step 11410 with the coupon information indicated on the coupon by verification of Step 1411.

[0208]Also in the electronic coupon system built over a 3rd embodiment as explained aboveThe digital signature of coupon information troubled like a 1st embodiment mentioned above if a serial numberthe term of validitythe amount of moneyetc. are alteredHe is trying to create the coupon which calculated using the secret key which is the information which only the issue-of-banknotes person 700 knowsand indicated the calculated digital signature as data which can be viewed.

[0209]Thereforelike [ according to the electronic coupon system concerning a 3rd embodiment ] a 1st embodiment mentioned aboveEven when the consumer 200 prints and uses an electronic couponforgery and an alteration of a coupon can be detected by verifying the digital signature indicated on the printed coupon.

[0210]Although the issue-of-banknotes person 700 who creates a digital signature differs from the vender 600 who verifies a digital signature in the electronic coupon system concerning a 3rd embodimentVerification of the digital signature according to the vender 600 by using the secret key of the issue-of-banknotes person 700 at the time of creation of a digital signatureand using the public key of the issue-of-banknotes person 700 at the time of verification of a digital signature is possible. Howevereven if coupon information is enciphered and it indicates the enciphered encipherment information on a coupon as data which can be viewed using the secret encryption key which only the both sides of the vender 600 and the issue-of-banknotes person 700 knowverification of the encipherment information by the vender 600 is possible.

[0211]He is trying to create the coupon which indicated the irreversible transformation value of the password which the consumer 200 presented as data which can be viewed like a 1st embodiment mentioned above also in the electronic coupon system concerning a 3rd embodiment at the time of the issue of banknotes of a coupon. He is trying to compare the irreversible transformation value of the password which showed the vender 600 the password which only the consumer 200 who demanded the issue of banknotes knowsand the consumer 200 presented with the irreversible transformation value indicated on the coupon at the time of use of a coupon.

[0212]Thereforeaccording to the electronic coupon system concerning a 3rd embodimentlike a 1st embodiment mentioned aboveeven if a coupon is stolenthe third party who does not know the password which the issue-of-banknotes demand of the coupon was shown can be prevented from using a coupon improperly.

[0213]In the electronic coupon system concerning a 3rd embodimentSince it is convenient even if the example which indicated about the password the irreversible transformation value which performed irreversible transformation on

the coupon as data which can be viewed is shownand it exhibits the irreversible transformation method according to this exampleVerification of the irreversible transformation value by the vender 600 is possibleand when the irreversible transformation value of a password is inharmoniousthe consumer 200 is able to calculate and check the irreversible transformation value of the password which self presented. Howevereven if it indicates about a password the encipherment information enciphered with the encryption method which can encipher only the both sides of the vender 600 and the issue-of-banknotes person 700 on a coupon as data which can be viewedverification of the encipherment information by the vender 600 is possible.

[0214]Also in the electronic coupon system concerning a 3rd embodimentas a 1st embodiment mentioned above explainedvarious modification is possible within the limits of the gist of this invention.

[0215]For examplein the electronic coupon system concerning a 3rd embodimentwhen transmitting a password to the issue-of-banknotes person 700 and the vender 600the consumer 200 acquires the public key of the issue-of-banknotes person 700 and the vender 600and is made to perform encryption communicationbut he does not limit this invention to this. The consumer 200 can use the public key after 2 timesif the public key of the issue-of-banknotes person 700 and the vender 600 comes to hand once. As long as it can have a common key between the issue-of-banknotes person 700 and the vender 600and the consumer 200it may be made to encipher using secret key cryptosystem art.

[0216]When transmitting a password from the consumer 200 to the issue-of-banknotes person 700 and the vender 600 in the electronic coupon system concerning a 3rd embodimentIn order that the enciphered password may prevent it being stolen as it is and used improperlya password is enciphered with other information (a random number and a suitable number may be sufficient.)and it may be made to transmit.

[0217]In the electronic coupon system concerning a 3rd embodimentalthough he is made to indicate a digital signature on a coupon as data of a numerical valuea characteretc. which can be viewedif viewing after printing is possible for the issue-of-banknotes person 700he needs a bar code etc.for example. If it indicates as a bar codewhen the vender 600 acquires a variety of information from the printed couponhe can use a bar code reader.

[0218]In the electronic coupon system concerning a 3rd embodimentalthough the issue-of-banknotes person 700 is made to indicate independently the irreversible transformation value of the consumer's 200 passwordand the digital signature of coupon informationsuch as a serial numberthe term of validityand the amount of moneyon a couponIt may be made for a password to also calculate a digital signature together with coupon information. After the information on the origin which calculates digital signaturessuch as coupon information and a passwordat this time performs irreversible transformationit may be made to calculate a digital signature.

[0219]Although how the vender 600 verifies the coupon in which use was

demanded from the consumer 200 in the electronic coupon system concerning a 3rd embodimentand the issue-of-banknotes person 700 manages in a unified manner and verifies only double use of a coupon is takenThe coupon which the vender 600 received is shown to the issue-of-banknotes person 700 with the password to which it was then shownand it may be made to verify a coupon by the issue-of-banknotes person 700 side. It may be made to combine the both.
[0220]If a coupon is verified by the issue-of-banknotes person 700 sidethe encipherment information which enciphered coupon information using the secret encryption key which only the issue-of-banknotes person 700 knows is indicated on a coupon as data which can be viewedand this encipherment information can be verified. The encipherment information which enciphered the password with the encryption method which can encipher only the issue-of-banknotes person 700 is indicated on a coupon as data which can be viewedand this encipherment information can be verified.
[0221]In the electronic coupon system concerning (a 4th embodiment) and a 3rd embodiment mentioned above in timethe issue-of-banknotes person 700As a 2nd embodiment mentioned above explaineda ticket can be dealt with and only a different point from a 2nd embodiment and a 3rd embodiment which mentioned above the case where it was made suchas a 4th embodiment is explained.
[0222]The outline composition of the electronic coupon system concerning a 4th embodiment is the same as the outline composition shown in drawing 26.
[0223]Drawing 34 is a figure showing the hardware constitutions of the issue-of-banknotes person terminal 701.
[0224]A different point from the hardware constitutions shown in drawing 27 is a point that the ticket issue of banknotes and the verification processing program 707c are temporarily stored in the memory 707.
[0225]The ticket issue of banknotes and the verification processing program 707c are programs for issuing a ticket to the consumer 200 or verifying the ticket in which use was demanded from the consumer 200.
[0226]The hardware constitutions of the seller terminal 601 are the same as the hardware constitutions shown in drawing 28and the hardware constitutions of the consumer terminal 201 are the same as the hardware constitutions shown in drawing 16.
[0227]Nextoperation of the electronic coupon system concerning a 4th embodiment is explained.
[0228]The consumer terminal 201 performs actually processing which the consumer 200 performs with the consumer's 200 directions like a 3rd embodiment that also mentioned following explanation **** aboveand the issue-of-banknotes person terminal 701 performs actually processing which the issue-of-banknotes person 700 performs with the issue-of-banknotes person's 700 directions.
[0229]Drawing 35 is a figure for explaining operation until the consumer 200 receives the 1st ticket that required the issue of banknotes of the 1st ticket of the issue-of-banknotes person 700and was issued by the issue-of-banknotes person 700. Only n tickets shall demonstrate effectwhen it collects.

[0230]In drawing 35firstthe consumer 200 performs the initial ticket issue-of-banknotes request process (S12100) mentioned laterand transmits the password 501 of the enciphered self to the issue-of-banknotes person 700.
[0231]The peculiar value ("UID" is called hereafter.) 505 given in order that the issue-of-banknotes person 700 might perform initial ticket ticket issue processing (S7100) mentioned later and might identify the group of n ticketsif the password 501 was receivedAlthough the secret information (for examplesecret key of the issue-of-banknotes person 700) which only the password 501 and UID505 which receivedand the issue-of-banknotes person 700 know was connectedn-th irreversible transformation value $H_n$ (506 $_n$) is transmitted to the consumer 200 as the 1st ticket.
[0232]If UID505 and $H_n$ (506 $_n$) are receivedthe consumer 200 will perform ticket reception (S12200) mentioned laterand will keep UID505 and $H_n$ (506 $_n$) which received.
[0233]It differs in that the vender 100 has replaced with the issue-of-banknotes person 700 the operation shown in drawing 35 in the operation shown in drawing 17.
[0234]Namelyalthough the processing flow chart of the initial ticket issue-of-banknotes request process (S12100) of drawing 35 is the same as the processing flow chart of the initial ticket issue-of-banknotes request process (S2100) shown in drawing 19The point of using the public key of the issue-of-banknotes person 700 instead of the vender's 100 public key differs from the point that the transmission destination of the enciphered password 501 becomes the issue-of-banknotes person 700 instead of the vender 100.
[0235]Although the processing flow chart of the initial ticket ticket issue processing (S7100) of drawing 35 is the same as the processing flow chart of the initial ticket ticket issue processing (S1100) shown in drawing 20The point (point that this processing is realized by the ticket issue of banknotes and the verification processing program 707c) that the issue-of-banknotes person 700 performs this processing differs from the point of using the secret key of the issue-of-banknotes person 700 instead of the vender's 100 secret key.
[0236]The processing flow chart of the ticket reception (S12200) of drawing 35 is the same as the processing flow chart of the ticket reception (S2200) shown in drawing 21.
[0237]Drawing 36 is a figure for explaining operation until the consumer 200 receives the ticket after the 2nd sheet that required the issue of banknotes of the ticket after the 2nd sheet of the issue-of-banknotes person 700and was issued by the issue-of-banknotes person 700.
[0238]In drawing 36firstwhen receiving the issue of banknotes of the 2nd ticketthe consumer 200The ticket issue-of-banknotes request process (S12300) mentioned later is performedand the password 501 of the enciphered selfand UID505 and $H_n$ (506 $_n$) which came to hand by the ticket reception (S12200) of the 1st sheet are transmitted to the issue-of-banknotes person 700.
[0239]If the issue-of-banknotes person 700 receives the password 501UID505and

$H_n$ (506 $_n$)The password 501 and UID505 which performed ticket ticket issue processing (S7200) mentioned laterand receivedand $H_n$ (506 $_n$)From the secret key of the issue-of-banknotes person 700$H_{n-1}$ (506 $_{n-1}$) is calculated and calculated $H_{n-1}$ (506 $_{n-1}$) is transmitted to the consumer 200 as the 2nd ticket.

[0240]Ticket reception (S122200) will be performed and the consumer 200 will keep $H_{n-1}$ (506 $_{n-1}$) which receivedif $H_{n-1}$ (506 $_{n-1}$) is received.

[0241]Similarlywhen receiving the issue of banknotes of the m+1st (1 <=m<n) ticketsthe consumer 200A ticket issue-of-banknotes request process (S12300) is performedand the password 501 of the enciphered selfand UID505 and $H_{n-(m-1)}$ ($506_{n-(m-1)}$) which came to hand by the ticket reception (S12200) of the m-th sheet are transmitted to the issue-of-banknotes person 700.

[0242]If the issue-of-banknotes person 700 receives the password 501UID505and $H_{n-(m-1)}$ ($506_{n-(m-1)}$)The password 501 and UID505 which performed ticket ticket issue processing (S7200)and receivedand $H_{n-(m-1)}$ ($506_{n-(m-1)}$)From the secret key of the issue-of-banknotes person 700$H_{n-m}$ (506 $_{n-m}$) is calculated and calculated $H_{n-m}$ (506 $_{n-m}$) is transmitted to the consumer 200 as the m+1st tickets.

[0243]Ticket reception (S122200) will be performed and the consumer 200 will keep $H_{n-m}$ (506 $_{n-m}$) which receivedif $H_{n-m}$ (506 $_{n-m}$) is received.

[0244]Thusfor the consumer 200 to be able to collect n tickets and demonstrate the effect of these n tickets. A ticket issue-of-banknotes request process (S12300) is performedand the password 501 of the enciphered selfand UID505 and $H_1$ (506 $_1$) which came to hand by the ticket reception (S12200) of the n-th sheet are transmitted to the issue-of-banknotes person 700.

[0245]If the issue-of-banknotes person 700 receives the password 501UID505and $H_1$ (506 $_1$)Ticket ticket issue processing (S7200) is performedand from the password 501 and UID505 which received$H_1$ (506 $_1$)and the secret key of the issue-of-banknotes person 700the consumer 200 checks having collected tickets and performs only n n ticket collection end processing (S7250).

[0246]It differs in that the vender 100 has replaced with the issue-of-banknotes person 700 the operation shown in drawing 36 in the operation shown in drawing 18.

[0247]Namelyalthough the processing flow chart of the ticket issue-of-banknotes request process (S12100) of drawing 36 is the same as the processing flow chart of the ticket issue-of-banknotes request process (S2300) shown in drawing 22It differs in that the transmission destination of the point of using the public key of the issue-of-banknotes person 700 instead ofthe enciphered password 501 and UID505 savedand $H_m$ becomes the issue-of-banknotes person 700 instead of the vender 100. [ the vender's 100 public key ]

[0248]Although the processing flow chart of the ticket ticket issue processing (S7100) of drawing 36 is the same as the processing flow chart of the ticket ticket issue processing (S1200) shown in drawing 23The point (point that this processing is realized by the ticket issue of banknotes and the verification processing program 707c) that the issue-of-banknotes person 700 performs this processing differs from the point of using the secret key of the issue-of-banknotes person

700 instead of the vender's 100 secret key.
[0249]The processing flow chart of the ticket reception (S12200) of drawing 36 is the same as the processing flow chart of the ticket reception (S2200) shown in drawing 21.
[0250]Although the effect demonstrated when only n tickets are collected can differ according to the vender's 100 sales policySince the issue-of-banknotes person 700 is made to judge whether only n tickets were collectedthe issue-of-banknotes person 700 shall perform ticket collection end processing (S7250) of drawing 36.
[0251]Also in the electronic coupon system built over a 4th embodiment as explained aboveLike a 2nd embodiment mentioned above from what connected UID for identifying the group of the secret key of the issue-of-banknotes person 700 who is the secret information which only the issue-of-banknotes person 700 knowsthe password which is the information which only the consumer 200 knowsand n tickets at the time of the issue of banknotes of a ticket. Repeatcalculate an irreversible transformation value and in n-th irreversible transformation value $H_n$the n-1st irreversible transformation value $H_{n-1}$--the turn of 2nd irreversible transformation value $H_2$ and 1st irreversible transformation value $H_1$. He is trying to reply each irreversible transformation value to the consumer 200. He is trying to transmit $H_m$ and UID which were transmitted from the consumer 200 1 time ago to the issue-of-banknotes person 700and a password. The data required to calculate an irreversible transformation value for every consumer 200 is made to be transmitted from the consumer 200 to the issue-of-banknotes person 700.
[0252]Thereforeeven if a ticket is stolen [ according to the electronic coupon system concerning a 4th embodiment ] on a channel like a 2nd embodiment mentioned above in addition to the effect by a 3rd embodiment mentioned aboveThe third party who does not know a password can be prevented from using a ticket improperlyand it becomes unnecessary to manage how many tickets were already issued every consumer 200 by the issue-of-banknotes person 700 side.
[0253]Also in the electronic coupon system concerning a 4th embodimentas a 3rd embodiment mentioned above explainedvarious modification is possible within the limits of the gist of this invention.
[0254]For examplein the electronic coupon system concerning a 4th embodimentalthough the issue-of-banknotes person 700 is made to calculate an irreversible transformation value by using the secret key of the issue-of-banknotes person 700 at the time of the ticket issue of banknotesSince this calculation is good if incalculable except issue-of-banknotes person 700if the algorithm of irreversible transformation is disclosureit is not necessary to use the secret key of the issue-of-banknotes person 700.
[0255]In the electronic coupon system concerning a 4th embodimentAlthough the issue-of-banknotes person 700 transmits UID to the consumer 200 at the time of the initial ticket issue of banknotesand the consumer 200 keeps the UID and is made to transmit kept UID from the consumer 200 to the issue-of-banknotes

person 700 after thatIt may be made to transmit UID from the issue-of-banknotes person 700 to the consumer 200 each time at the time of the ticket issue of banknotes.

[0256]Although the issue-of-banknotes person 700 is made to reply the irreversible transformation value calculated from the secret key of the issue-of-banknotes person 700the passwordand the thing that connected UID at the time of the ticket issue of banknotes to the consumer 200 in the electronic coupon system concerning a 4th embodimentWhat connected a password and UID is enciphered using the secret encryption key (for examplesecret key of the issue-of-banknotes person 700 in a public-key crypto system) which only the issue-of-banknotes person 700 knowsand it may be made to reply the enciphered encipherment information to the consumer 200. The issue-of-banknotes person 700 in detail based on encipherment information $H_1$ of what connected a password and UIDEncipherment information $H_{i+1}$ of encipherment information $H_i$ ($1 <= i < n$) is calculated one by oneIt may be made to reply each encipherment information to the consumer 200 in n-th encipherment information $H_n$the n-1st encipherment information $H_{n-1}$--the turn of 2nd encipherment information $H_2$ and 1st encipherment information $H_1$.

[0257]Although the issue-of-banknotes person 700 is made to reply the irreversible transformation value calculated from the secret key of the issue-of-banknotes person 700the passwordand the thing that connected UID at the time of the ticket issue of banknotes to the consumer 200 in the electronic coupon system concerning a 4th embodimentWhat connected the number-of-sheets information which shows a passwordUIDand the how many ticket it isIt enciphers using the secret encryption key (for examplesecret key of the issue-of-banknotes person 700 in a public-key crypto system) which only the issue-of-banknotes person 700 knowsand may be made to reply the enciphered encipherment information to the consumer 200. If it does in this waythe issue-of-banknotes person 700 can know how many tickets the consumer 200 collected using the number-of-sheets information acquired as a result of decoding the encipherment information transmitted to the issue-of-banknotes demand of a ticket using the secret encryption key which only the issue-of-banknotes person 700 knows from the consumer 200.

[0258]In the electronic coupon system concerning a 4th embodimentalthough the issue-of-banknotes person 700 is made to transmit an irreversible transformation value to the consumer 200 at the time of the ticket issue of banknotesThe ticket indicated as data which can view an irreversible transformation value as well as the coupon explained by a 1st embodiment mentioned above is createdand it may be made to transmit the ticket as a document to the consumer 200.

[0259]Like the coupon explained by a 1st embodiment mentioned above also in the electronic coupon system concerning a 4th embodimentfrom the issue-of-banknotes person 700 to the consumer 200 with a ticket. If the digital signature of the whole ticket may be made to be transmitted and it does in this wayit is verifiable whether the received ticket is altered by the consumer 200 side who

received the issue of banknotes of the ticket.
[0260]
[Effect of the Invention]Since the unauthorized use of the coupon by forgery of a couponan alterationand a third party can be detected even when the coupon issued electronically is printed and used according to this inventionas explained aboveConsumers can use now the coupon issued electronically not only in the virtual store established on the network but in the store which exists actually.
[0261]According to this inventionsince it becomes unnecessary to manage consumers by the side which issues a ticket when only two or more sheets are collected and it deals with the ticket which demonstrates effectthe time and effort of the side which issues a ticket can be reduced.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The outline lineblock diagram of the electronic coupon system concerning a 1st embodiment.
[Drawing 2]The hardware-constitutions figure of the seller terminal in a 1st embodiment.
[Drawing 3]The hardware-constitutions figure of the consumer terminal in a 1st embodiment.
[Drawing 4]The explanatory view of operation until consumers receive the coupon which required the issue of banknotes of the coupon of the venderand was issued by the vender among operations of the electronic coupon system concerning a 1st embodiment.
[Drawing 5]The explanatory view of operation until the consumers who have already received the issue of banknotes of the coupon among operations of the electronic coupon system concerning a 1st embodiment use a coupon via a communications network and a vender verifies a coupon.
[Drawing 6]The explanatory view of operation until the consumers who have already received the issue of banknotes of the coupon among operations of the electronic coupon system concerning a 1st embodiment print a couponand bring and use the printed coupon for a store and a vender verifies a coupon.
[Drawing 7]The processing flow chart of the coupon request process of drawing 4.
[Drawing 8]The processing flow chart of the coupon ticket issue processing of drawing 4.
[Drawing 9]The processing flow chart of the coupon reception of drawing 4.
[Drawing 10]The processing flow chart of coupon use on-line processing of drawing 5.
[Drawing 11]The processing flow chart of coupon use off-line processing of drawing 6.
[Drawing 12]Drawing 5 and the processing flow chart of the coupon verification processing of drawing 6.

[Drawing 13]The processing flow chart of the document verification processing performed at Step 1404 of drawing 12.
[Drawing 14]The explanatory view showing an example of the form of the coupon issued with the electronic coupon system concerning a 1st embodiment.
[Drawing 15]The hardware-constitutions figure of the seller terminal in a 2nd embodiment.
[Drawing 16]The hardware-constitutions figure of the consumer terminal in a 2nd embodiment.
[Drawing 17]The explanatory view of operation until consumers receive the 1st ticket that required the issue of banknotes of the 1st ticket of the venderand was issued by the vender among operations of the electronic coupon system concerning a 2nd embodiment.
[Drawing 18]The explanatory view of operation until consumers receive the ticket after the 2nd sheet that required the issue of banknotes of the ticket after the 2nd sheet of the venderand was issued by the vender among operations of the electronic coupon system concerning a 2nd embodiment.
[Drawing 19]The processing flow chart of the initial ticket issue-of-banknotes request process of drawing 17.
[Drawing 20]The processing flow chart of the initial ticket ticket issue processing of drawing 17.
[Drawing 21]Drawing 17 and the processing flow chart of the ticket reception of drawing 18.
[Drawing 22]The processing flow chart of the ticket issue-of-banknotes request process of drawing 18.
[Drawing 23]The processing flow chart of the ticket ticket issue processing of drawing 18.
[Drawing 24]The explanatory view showing signs that an irreversible transformation value is calculated at Step 1105 of drawing 20.
[Drawing 25]The explanatory view showing an example of a display with the consumer terminal in a 2nd embodiment.
[Drawing 26]The outline lineblock diagram of the electronic coupon system concerning a 3rd embodiment.
[Drawing 27]The hardware-constitutions figure of the issue-of-banknotes person terminal in a 3rd embodiment.
[Drawing 28]The hardware-constitutions figure of the seller terminal in a 3rd embodiment.
[Drawing 29]The explanatory view of operation until consumers receive the coupon which required the issue of banknotes of the coupon of the issue-of-banknotes personand was issued by the issue-of-banknotes person among operations of the electronic coupon system concerning a 3rd embodiment.
[Drawing 30]The explanatory view of operation until the consumers who have already received the issue of banknotes of the coupon among operations of the electronic coupon system concerning a 3rd embodiment use a coupon via a communications network and a vender verifies a coupon.

[Drawing 31]The explanatory view of operation until the consumers who have already received the issue of banknotes of the coupon among operations of the electronic coupon system concerning a 3rd embodiment print a couponand bring and use the printed coupon for a store and a vender verifies a coupon.
[Drawing 32]Drawing 30 and the processing flow chart of the coupon verification processing of drawing 31.
[Drawing 33]The processing flow chart of the document verification processing performed at Step 11404 of drawing 32.
[Drawing 34]The hardware-constitutions figure of the issue-of-banknotes person terminal in a 4th embodiment.
[Drawing 35]The explanatory view of operation until consumers receive the 1st ticket that required the issue of banknotes of the 1st ticket of the issue-of-banknotes personand was issued by the issue-of-banknotes person among operations of the electronic coupon system concerning a 4th embodiment.
[Drawing 36]The explanatory view of operation until consumers receive the ticket after the 2nd sheet that required the issue of banknotes of the ticket after the 2nd sheet of the issue-of-banknotes personand was issued by the issue-of-banknotes person among operations of the electronic coupon system concerning a 4th embodiment.
[Description of Notations]
100600 -- A vender200 $_1$ - 200 $_n$ -- Consumers700 -- An issue-of-banknotes person101601 $_1$ - 601 $_n$ -- Seller terminal201 $_1$ - 201 $_n$ -- A consumer terminal701 -- Issue-of-banknotes person terminal300 -- A communications network102202702 -- Communications network interface103203703 -- A display104204704 -- Input device105205705 -- Memory storage106206706 -- Central processing unit (CPU)107207707 -- A temporary memory (memory)208 -- Printer110210710 -- A bus107a207a707a -- Operating system (OS)107b707b -- The coupon issue of banknotes and a verification processing program107c707c -- The ticket issue of banknotes and a verification processing program207b -- A coupon demandreception and a calling processing program607b -- Coupon verification processing program207c [ -- A digital signature504 / -- The coupon505 which were printed / -- UID506 $_1$ - 506 $_n$ / -- An irreversible transformation value507 / -- Secret key. ] -- A ticket demandreception and a calling processing program501 -- A password502 -- A coupon503